mca net

digicon

SISTEMA DE ACESSO

MANUAL DO USUÁRIO

Modo de utilização e funcionalidades

digicon

EMPRESA ISO 9001:2000 CERTIFICADA

SEDE: Rua Nissin Castiel, 640 • Distrito Industrial
Cep: 94000-970 • Gravataí • RS • Brasil
Fone: +55 51 3489.8737

FILIAL: Rua São Paulo, 82 • Alphaville
Cep: 06465-130 • Barueri • SP
Fone: +55 11 4133.4100 • Fax: + 55 11 4191.2585

e-mail: vendas.acesso@digicon.com.br
www.digicon.com.br

A DIGICON reserva-se o direito de alterar as características destes equipamentos sem aviso prévio.

+DI.0XX.01-Mai/09

Revisões

Nº da revisão	Descrição da revisão	Data	Responsável
1.0	Criação	01/02/2010	Gustavo Pinheiro e Sousa
1.1	Ajuste de template e revisão	20/04/2010	João Marcelo T. e S. Torres

2 Sumário

1 Revisões 3

2 Sumário 4

3 Índice de Ilustrações 7

4 Conteúdo da caixa 11

5 Especificações técnicas 12

6 Apresentação 13

7 Instalação e Cuidados 17

7.1 Instalação física 17

7.1.1 Fixação Utilizando caixa metálica 19

7.1.2 Fixação utilizando caixa 2x4 21

7.1.3 Botão 22

7.1.4 Solenóides 22

7.1.5 Cabo Ethernet 22

7.2 Começando a utilizar o dispositivo 22

8 Descrição do equipamento 23

9 Utilização 24

9.1 Utilizando os dispositivos de autorização 26

9.1.1 Sensor Biométrico de Digitais 26

9.1.2 Leitor de Código de Barras 26

9.1.3 Leitor de Cartão Mifare e RFID 27

9.1.4 Teclado Capacitivo 27

9.2 Entrada USB 28

9.3 Navegando nos Menus 29

9.4 Menu do Usuario 30

9.5 Menu do Técnico 31

9.6 Menu do Operador 33

9.7 Menu do Administrador 35

9.8 Atualização de firmware do dispositivo 37

9.9 Descrição dos Menus e Funções 38

9.10 Menu Configuração 38

9.10.1 Menu Sistema 38

9.10.1.1 Memória RAM 38

9.10.1.2 Módulos de Sistema 38

9.10.1.3 Versão do Sistema 38
9.10.1.4 Armazenamento 39
9.10.1.5 Versão Aplicativo 39
9.10.2 Alterar língua 39
9.10.3 Menu Data/Hora 40
9.10.3.1 Alterar Data/Hora 40
9.10.3.2 Visualizar Data/Hora 40
9.10.3.3 Menu Horário de Verão 41
9.10.3.3.1 Excluir Horário de Verão 41
9.10.3.3.2 Cadastrar Horário de Verão 41
9.10.3.3.3 Visualizar Horário de Verão 42
9.10.4 Menu REDE 42
9.10.4.1 Mostrar IP 42
9.10.4.2 IP Dinâmico 42
9.10.4.3 IP Estático 43
9.10.5 Max. Usuários 43
9.10.6 Timeouts 43
9.10.7 Menu Limpeza 44
9.10.7.1 Apagar Logs 44
9.10.7.2 Resetar Hardware 45
9.10.8 Conf. Período 45
9.10.9 Chave MIFARE 47

9.11 Menu Operação 47
9.11.1 Dispositivos de Autorização 48
9.11.2 Modo de Operação 48
9.11.3 Menu Saídas 49
9.11.3.1 Botão 49
9.11.3.2 Fechadura 50
9.11.3.3 Auxiliar 51
9.11.4 Menu Auditoria 53
9.11.4.1 Habilitar Auditoria 53
9.11.4.2 Maximo de eventos 53
9.11.4.3 Limpeza de eventos 54
9.11.5 Status da porta 54
9.11.6 Menu Tela Principal 55
9.11.6.1 Nome Empresa 55
9.11.6.2 Mensagem Tela 56
9.11.7 ID do equipamento 56
9.11.8 Beep Teclado 57
9.11.9 Soft Reset 58
9.11.10 Menu Backup 58
9.11.10.1 Criar Backup 58
9.11.10.2 Restaurar Backup 60

9.12 Menu Cadastro 61
9.12.1 Menu Usuário 61
9.12.1.1 Seleção de usuários 61
9.12.1.2 Menu Incluir 62
9.12.1.2.1 ID/Senha 62
9.12.1.2.2 Biometria 64

9.12.1.2.3 Código de Barras 65
9.12.1.2.4 RFID 65
9.12.1.2.5 MIFARE 66
9.12.1.2.6 MIFARE+Biometria 66
9.12.1.2.7 Horário de Visita 67
9.12.1.3 Menu Deletar 67
9.12.1.3.1 ID/Senha 68
9.12.1.3.2 Biometria 68
9.12.1.3.3 Código de Barras 68
9.12.1.3.4 RFID 68
9.12.1.3.5 MIFARE 68
9.12.1.3.6 Horário de Visita 69
9.12.1.4 Menu Alterar 69
9.12.1.4.1 Menu Password 69
9.12.1.4.1.1 Usuario atual 69
9.12.1.4.1.2 Outro Usuario 70
9.12.1.4.2 Status 70
9.12.1.4.3 Perfil 71
9.12.1.4.4 Nome 72
9.12.1.4.5 Período de Acesso 73
9.12.2 Menu Datas 74
9.12.2.1 Agendar Configuração 74
9.12.2.2 Feriado 75

9.13 Menu Listas 76
9.13.1 Ponto/Acesso 76
9.13.2 Limpar Ponto/Acesso 77
9.13.3 Auditoria 78

10 Resolução de Problemas 80

10.1.1.1 Dispositivo não liga 80
10.1.1.2 Acionamento das saídas não funciona 80
10.1.1.3 Acesso negado em usuário cadastrado 80
10.1.1.4 Botao não funciona 80
10.1.1.5 Falha ao conseguir IP 81
10.1.1.6 Data e Hora errados 81
10.1.1.7 O acesso é permitido mas a porta não abre 81
10.1.1.8 Ao realizar uma operação envolvendo um dispositivo de armazenamento USB o dispositivo trava na tela "RETIRE O PENDRIVE" 81

3 Índice de Ilustrações

Figura 1 - Caixa 11
Figura 2 - MCANet 12
Figura 12 - Frente do dispositivo 23
Figura 13 - Acesso aos menus e ao local 24
Figura 14 – ACESSO - Acesso permitido e acesso negado 24
Figura 15 – MENU - Acesso permitido e acesso negado 25
Figura 16 - Modo de utilização do sensor biométrico 26
Figura 17 - Utilizando o leitor de código de Barras 26
Figura 18 - Utilização dos leitores sem contato 27
Figura 19 - Utilização do teclado Capacitivo 27
Figura 20 - Entrada USB 28
Figura 21 - Tela do Menu 29
Figura 22 - Menu do Usuário 30
Figura 23 - Menu do Técnico 31
Figura 24 - Menu do Operador 34
Figura 25 - Menu do Administrador 35
Figura 26 - Consulta da memória RAM 38
Figura 27 - Consulta dos módulos do sistema 38
Figura 28 - Versão do sistema Operacional 39
Figura 29 - Consulta de Armazenamento 39
Figura 30 - Versão do aplicativo 39
Figura 31 - Seleção de linguagem 39
Figura 32 - Confirmação de exclusão de horário de verão 40
Figura 33 - Tela de alteração de data/hora 40
Figura 34 - Confirmação de exclusão de horário de verão 40
Figura 35 - Visualização de data/hora 41
Figura 36 - Confirmação de exclusão de horário de verão 41
Figura 37 - Cadastro de horário de verão 41
Figura 38 - Visualização de horário de verão 42
Figura 39 - Visualização de endereço de rede do dispositivo 42
Figura 40 – Configuração de acesso á rede com IP Dinâmico 42
Figura 41 – Configuração de acesso á rede com IP Estático 43
Figura 42 – Confirmação de acesso á rede com IP Estático 43
Figura 43 – Configuração de número de usuários 43
Figura 44 – Configuração de Timeouts 44
Figura 45 – Confirmação de alteração de timeouts 44

Figura 46 – Limpeza dos Logs 45
Figura 47 – Confirmação de Resetar Hardware 45
Figura 48 – Configuração de período – dias da semana 45
Figura 49 – Configuração de período – hora início 46
Figura 50 – Configuração de período – hora fim 46
Figura 51 – Configuração de período – expiração 46
Figura 52 – Configuração de período – Tempo para expiração 47
Figura 53 – Entrada de chave dos cartões MIFARE 47
Figura 54 – Tela de confirmação da alteração de chave do MIFARE 47
Figura 55 – Seleção de dispositivos de autorização 48
Figura 56 – Tela de confirmação da alteração de dispositivos de operação 48
Figura 57 – Tela de seleção de modo de acesso 48
Figura 58 – Tela de confirmação da alteração de modo de operação 49
Figura 59 – Tela de configuração do botão 49
Figura 60 – Tela de confirmação da alteração de acionamento de botao 50
Figura 61 – Tela de escolha do estado da fechadura 50
Figura 62 – Tela de escolha do solenóide da fechadura 50
Figura 63 – Tempo de acionamento da fechadura 51
Figura 64 – Tela de confirmação da configuração da fechadura 51
Figura 65 – Tela de configuração da saída auxiliar 51
Figura 66 – Tela de escolha do estado da saída auxiliar 52
Figura 67 – Tela de configuração do tempo de acionamento da saída auxiliar 52
Figura 68 – Tela de confirmação da configuração da auxiliar 52
Figura 69 – Tela de configuração do tempo de acionamento da saída auxiliar 53
Figura 70 – Tela de confirmação da configuração da auxiliar 53
Figura 71 – Tela de configuração do Máximo de eventos 54
Figura 72 – Tela de confirmação da configuração da auxiliar 54
Figura 73 – Tela de confirmação da limpeza de eventos de auditoria 54
Figura 74 – Tela de status da porta 55
Figura 75 – Tela Inicial 55
Figura 76 – Tela de alteração do nome da empresa 55
Figura 77 – Tela de confirmação de alteração do nome de empresa 56
Figura 78 – Tela de alteração de mensagem 56
Figura 79 – Tela de confirmação de alteração de mensagem de tela 56
Figura 80 – Tela de alteração de Id do equipamento 57
Figura 81 – Tela de confirmação de alteração de Id do equipamento 57
Figura 82 – Tela de confirmação de alteração de Id do equipamento 58
Figura 83 – Tela de confirmação de alteração de Id do equipamento 58
Figura 84 – Tela de confirmação de reset da aplicação 58

Figura 85 – Tela de confirmação de criação de backup 59
Figura 86 – Tela de sucesso na realização do backup 59
Figura 87 – Tela de confirmação de restauração de backup 60
Figura 88 – Tela de sucesso na realização da restauração 61
Figura 89 – Tela de opção de escolha de usuário 61
Figura 90 – Lista de escolha de usuário 61
Figura 91 – Escolha de usuário por ID 62
Figura 92 – Dispositivo não instalado 62
Figura 93 –Biometria já cadastrada 62
Figura 94 – Tela de escolha do perfil 63
Figura 95 – Tela de escolha do ID de usuário 63
Figura 96 – Tela de escolha do nome de usuário 64
Figura 97 – Cadastro da primeira digital 64
Figura 98 – Cadastro da segunda digital 64
Figura 99 – Requisição de retirada do dedo do sensor 65
Figura 100 – Tela de cadastro de Código de barras 65
Figura 101 – Tela de cadastro de RFID 65
Figura 102 – Tela de cadastro de MIFARE 66
Figura 103 – Tela de captura de modelo de biometria 66
Figura 104 – Tela de gravação de biometria no MIFARE 67
Figura 105 – Tela de escolha da data para visita 67
Figura 106 – Tela de escolha da hora inicial da visita 67
Figura 107 – Tela de escolha da hora inicial da visita 67
Figura 108 – Confirmação de exclusão de usuário 68
Figura 109 – Tela de escolha de datas de visita 69
Figura 110 – Confirmação de exclusão de visita 69
Figura 111 – Alteração da própria senha de usuário 69
Figura 112 – Confirmação de alteração da própria senha de usuário 70
Figura 113 – Alteração de senha de usuário 70
Figura 114 – Confirmação de alteração de senha de usuário 70
Figura 115 – Alteração de senha de usuário 71
Figura 116 – Confirmação de alteração de senha de usuário 71
Figura 117 – Tela de escolha do perfil 71
Figura 118 – Confirmação de alteração de senha de usuário 72
Figura 119 – Alteração de nome de usuário 72
Figura 120 – Confirmação de alteração de nome de usuário 72
Figura 121 – Configuração de período – dias da semana 73
Figura 122 – Configuração de período – hora início 73
Figura 123 – Configuração de período – hora fim 73

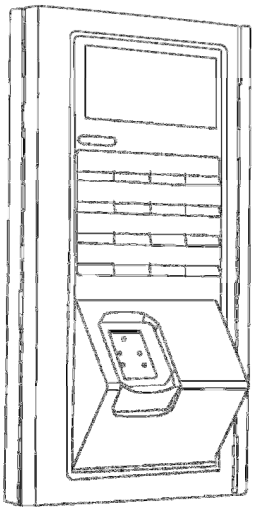
Figura 124 – Configuração de período – expiração 74
Figura 125 – Configuração de período – Data para expiração 74
Figura 126 – Agendamento de manutenção – Data e hora de início 74
Figura 127 – Agendamento de manutenção – Data e hora de início 75
Figura 128 – Confirmação de Agendamento de manutenção 75
Figura 129 – Agendamento de manutenção – Data e hora de início 75
Figura 130 – Agendamento de manutenção – Data e hora de início 76
Figura 131 – Confirmação de Agendamento de manutenção 76
Figura 132 – Tela de confirmação de gravação de lista de ponto/acesso 76
Figura 133 – Tela de sucesso na realização da gravação da lista de ponto/acesso 77
Figura 134 – Tela de confirmação de exclusão de eventos de ponto/acesso 78
Figura 135 – Tela de confirmação de gravação de lista de auditoria 79
Figura 136 – Tela de sucesso na realização da gravação da lista de auditoria 79

4 Conteúdo da caixa

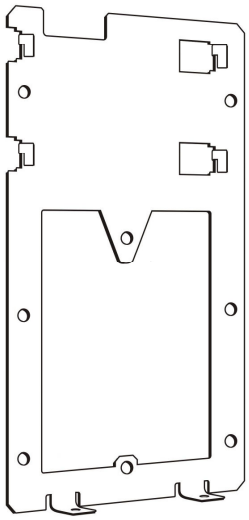
- Mcanet
- Suporte de parede liso
- Conjunto de parafusos para fixação
- Fonte de alimentação
- Manual

Figura 1 - Caixa

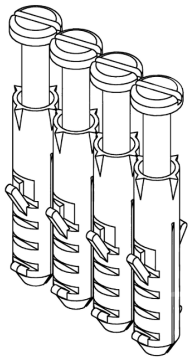
O conteúdo da caixa é mostrado a seguir para familiarização com os componentes:



MCANet



Suporte Liso



Conjunto de parafusos

Figura 2 – Conteúdo da caixa

5 Especificações técnicas

O dispositivo de acesso MCANet possui as seguinte características:

- Processador ARM-9 150MHz
- Memória Flash de 1MB a 32MB
- Memória RAM 32MB, 32 bits (opcional até 64MB, 16 bits)
- RTC (Circuito do relógio de grande precisão)
- *Tamper detection (Dispositivo que Gera Alarme de Violação com Registro de Horario)*
- Mifare, RFID, Barras e Biometria
- Ethernet 10/100 T ou USB
- 2 RS-485 (rede de comunicação e periféricos)
- 2 Entradas opto-isoladas
- 1Saída relé
- Saídas a transistor (coletor aberto)
- Saída Wiegand
- Display gráfico 128 x 64 pontos
- Teclado capacitivo de 16 teclas
- Sinalizador sonoro (beep)
- Pictograma com led bicolor
- Alimentação 12 VDC
- Alimentação POE

Figura 3 - MCANet

6 Apresentação

O sistema de Acesso Mcanet é uma solução completa para o controle de acesso a ambientes, possuindo várias formas de acesso sofisticadas e de fácil utilização, como:

- Entrada de senha via teclado;
- Reconhecimento biométrico (digitais);
- Leitura de cartões sem contato (MIFARE e RFId);
- Cartão com contato com código de barras;

De fácil utilização e de simples instalação ele lhe oferece maior segurança e administração dos locais desejados gerando um banco de dados contendo informações sobre a entrada de indivíduos na localidade monitorada e armazenamneto de eventos relativos ao uso do dispositvo.

Possui um sistema de permissionamento, permitindo restringir o nível de acesso dado a cada usuário cadastrado, de acordo com sua função ou necessidade. Os tipos de usuários que podem ser cadastrados organizam-se da seguinte forma:

- Usuário padrão – Usuário para acesso simples. Um individuo cadastrado como usuário pode abrir a porta guardada pela MCANet, e este nível de acesso pode ser combinado com qualquer um dos outros perfis, de forma a permitir que o mesmo possa além de ter acesso ao local, também acessar ao menu de configurações avançado.

- Técnico – O técnico cadastrado pode acessar o dispositivo para executar tarefas menores, como a coleta de dados do dispositivo. Possui restrição de horário, podendo acessar o menu somente em horário previamente cadastrado.

- Operador – Um operador possui acesso quase completo a todas as configurações do sistema, porém não possui poderes para editar as configurações de auditoria.

- Administrador - Possui poderes plenos, podendo alterar todas as configurações do sistema.

Cada MCANet pode ter vários dispositivos de acesso, assumindo várias combinações de meios de acesso, habilitando ou não cada um dos dispositivos presentes e dando maior flexibilidade na configuração de acesso.

6.1 Modelos disponíveis

O MCANet possui uma arquitetura modular, permitindo que vários modelos sejam disponibilizados, cada um com uma gama de dispositivos de autorização.

As tecnologias de autorização disponíveis são:

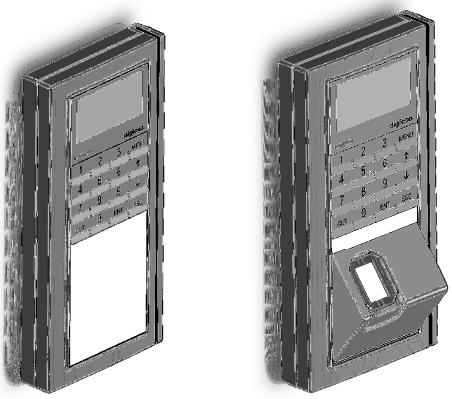


Figura 4 - MCANet barras, e MCANet barras com biometria

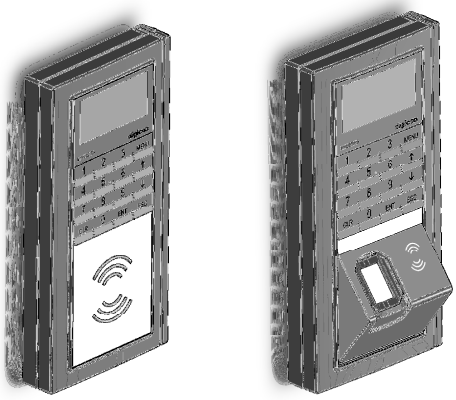


Figura 6 - MCANet Proximidade e MCANet Proximidade com biometria

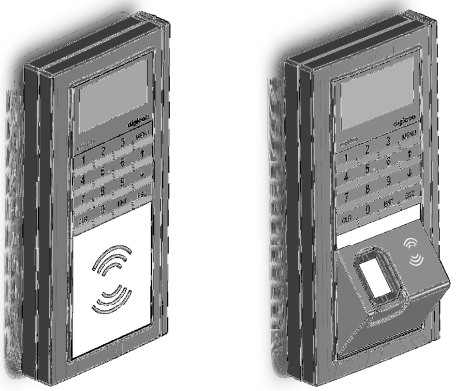


Figura 5 - MCANet MIFARE e MCANet MIFARE com biometria

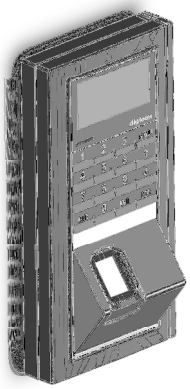


Figura 7 - MCANet biometria

Todos os modelos são capazes de autenticação via teclado através de senha fornecida pelo usuário.

Também estão disponíveis várias cores de moldura, para melhor adequação ao ambiente de utilização.

Figura 8 - Molduras disponíveis para o MCANet

Opção 1 – Moldura em cinza claro com painéis de leitura biométrica e teclado em preto

Opção 2 - Moldura colorida com painel de leitura de cartão e teclado em cinza claro

Opção 3 – Moldura em cinza escuro com painéis de leitura biométrica e teclado em preto.

6.2 Itens Opcionais

Existem ainda itens opcionais que podem ser adquiridos separadamente para melhor adequar o MCANet ao seu caso de uso.

Dentre estes itens temos:

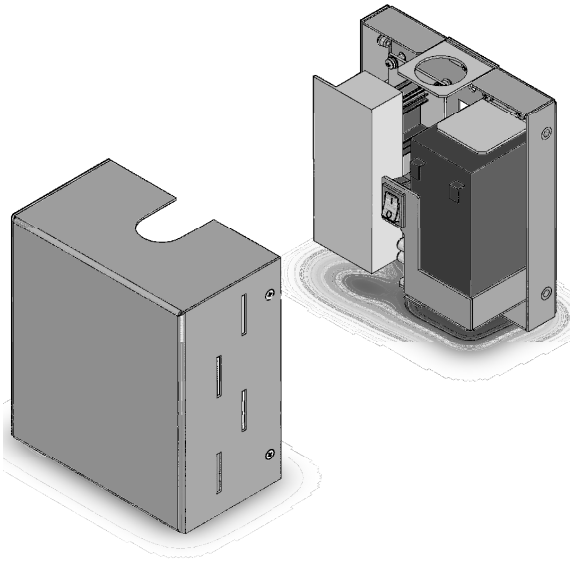


Figura 9 – Nobreak

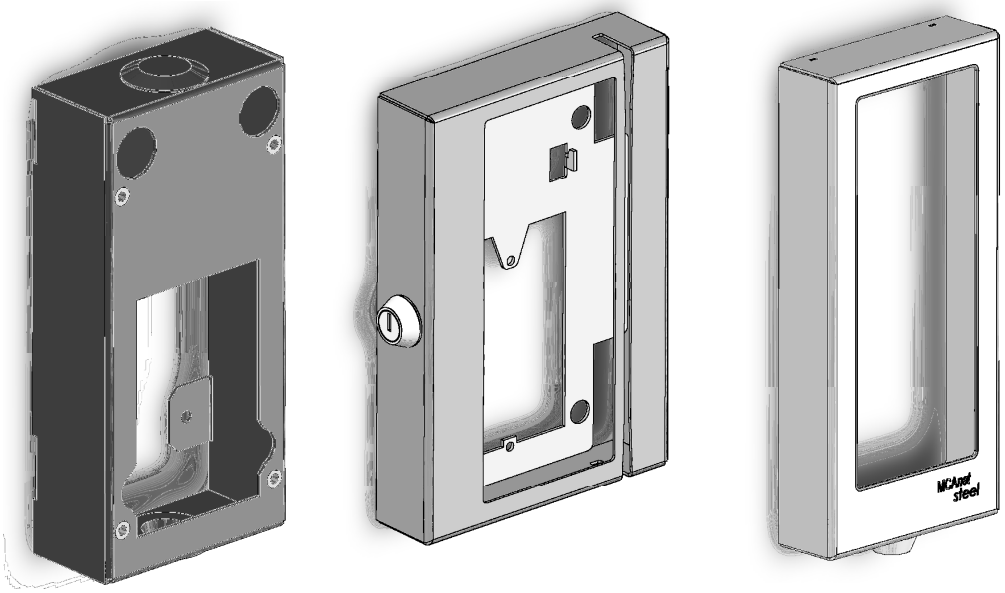


Figura 10 - Caixa metálica para instalação com eletrodutos e caixa de proteção com e sem vão para código de barras

O Nobreak é capaz de manter o MCANET em funcionamento em casos de falta de energia, evitando a quebra de segurança e impedimento de acesso nestes casos.

A caixa metálica serve para a instalação do seu MCANet em locais aonde não se encontra disponível cabeamento estruturado, protegendo a fiação da exposição ao ambiente.

A caixa de proteção foi projetada para a utilização do MCANet em ambientes de maior risco, impedindo que o equipamento seja danificado sem impedir sua utilização, e vem em dois modelos, um com vão para código de barras e outro mais compacto para utilização em dispositivos sem código de barras.

7 Instalação e Cuidados

No interior da caixa, será encontrado um suporte liso para fixação do dispositivo em uma parede ou suporte e uma caixa metálica para instalação utilizando eletrodutos. Recomenda-se que o usuário primeiramente faça a fixação dos suportes do modo apropriado para depois proceder com o cabeamento.

O MCANet possui um sensor de violação, não permitindo que o mesmo funcione caso o sensor esteja violado ou fora de seu suporte. Para tanto, recomenda-se que o usuário configure o dispositivo após sua devida fixação e instalação dos cabos.

7.1 Instalação física

Para melhor utilização do dispositivo, é recomendado que o usuário siga as recomendações abaixo.

Na instalação do dispositivo devem ser seguidas algumas distâncias de segurança, para conforto quando forem efetuadas as operações de autorização, navegação e utilização da porta USB.

As distâncias recomendadas são a 1,20 m de altura e 20 cm de distância da porta aonde será instalado o equipamento, com o ilustrado abaixo:

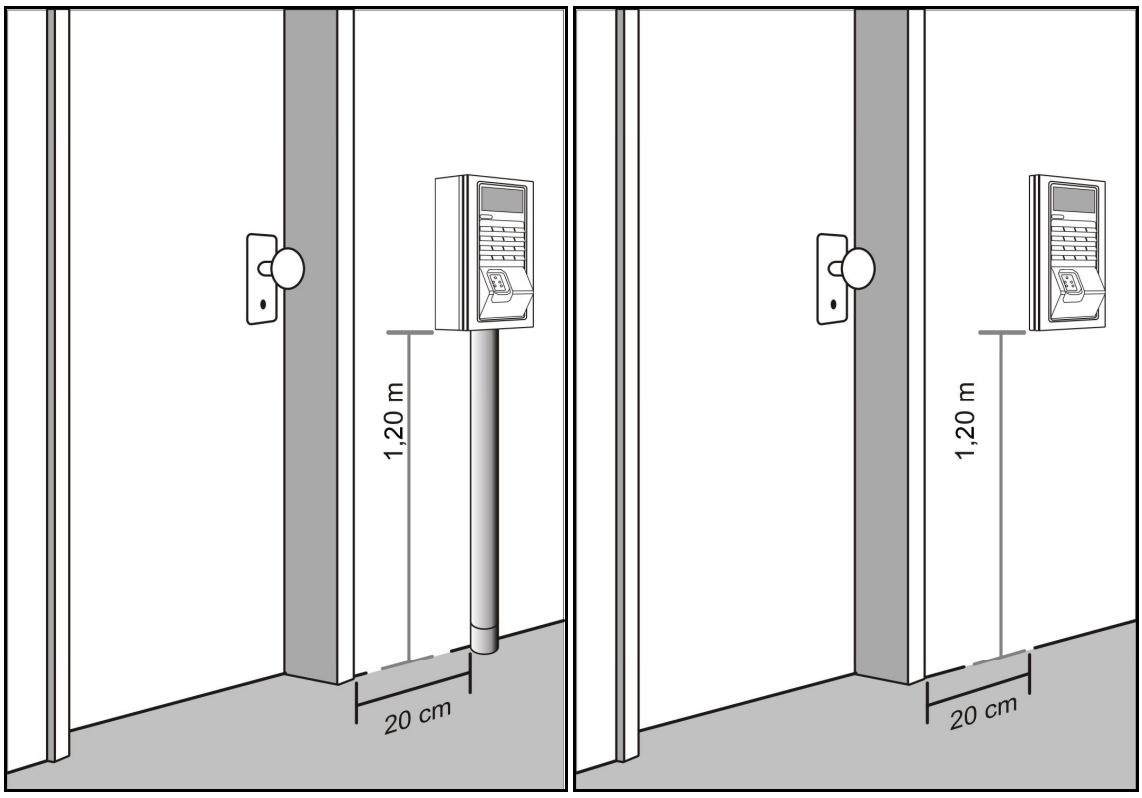


Figura 11 - Instalação dos dispositivos - distâncias mínimas

A instalação do dispositivo pode ser feita de duas maneiras como citado acima:

- Utilizando a caixa metálica, para instalação em locais aonde não há a possibilidade de utilização de cabeamento estruturado, e os cabos são passados através de eletrodutos.

- Utilizando a abertura do shaft da construção, na abertura 2x4 para passagem de cabeamento estruturado.

Nas próximas seções são detalhados ambos os modelos de instalação, para que o usuário escolha o mais apropriado a seu uso.

No verso do dispositivo temos os conectores aonde serão inseridos os cabos e conexões necessários ao seu funcionamento.

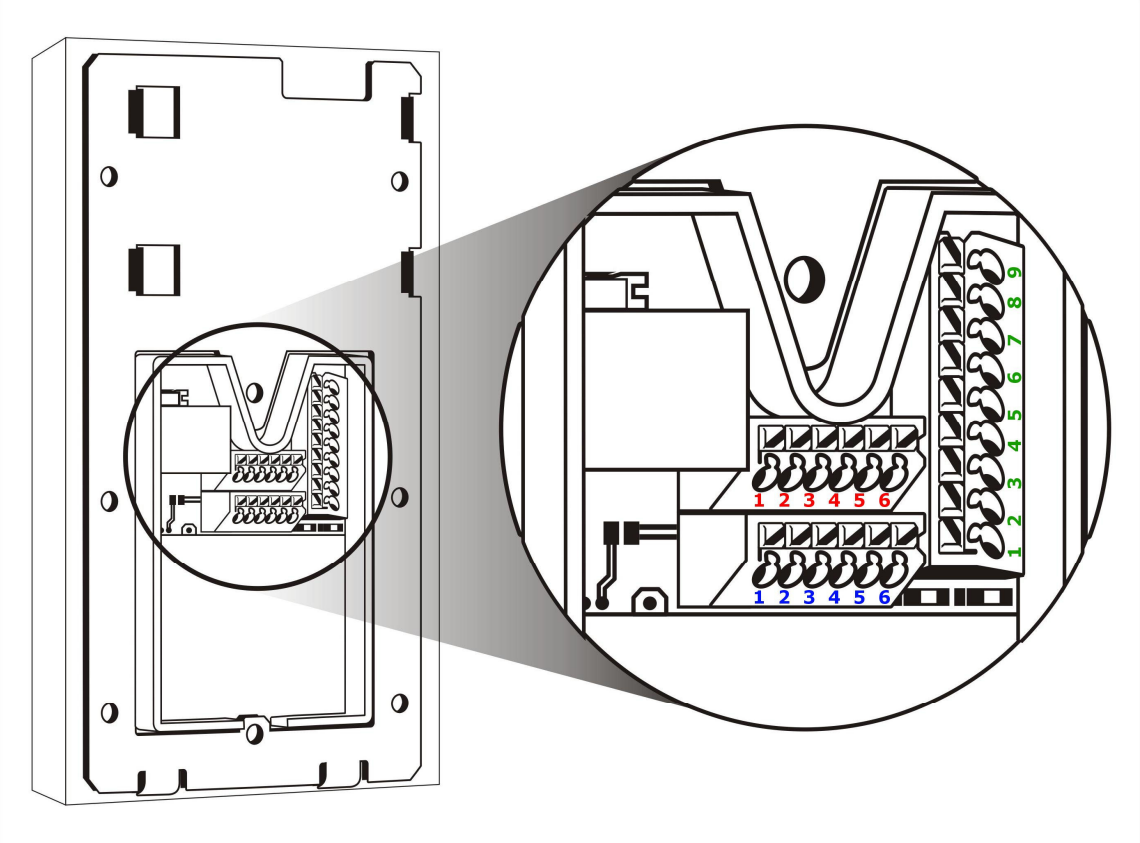


Figura 12 – Conectores

A numeração indicada tem a seguinte legenda:

1- Vin+ (12V positivo da fonte)
2- Vin- (Negativo da fonte)
3- Perif - Saída 12V
4- Perif - DORI
5- Perif - nDORI
6- Perif - GND
1- Relé - Comum
2- Relé - Saída (N.A.)
3- Entrada opto. 0
4- Entrada opto. 1
5- Opto. V+
6- Opto. GND
1- Solenóide - Saída 12V
2- Saída solenóide 0
3- Saída solenóide 1
4- RS485 - GND
5- RS485 - DORI
6- RS485 - nDORI
7- Saída wieg. - GND
8- Saída wieg - Data 0
9- Saída wieg - Data 1

Mais adiante serão mostrados alguns modelos de conexões mais recorrentes.

7.1.1 Tubulações

7.1.2 Fixação Utilizando caixa metálica

A instalação do dispositivo com a utilização da caixa metálica pode ser feita em 4 passos:

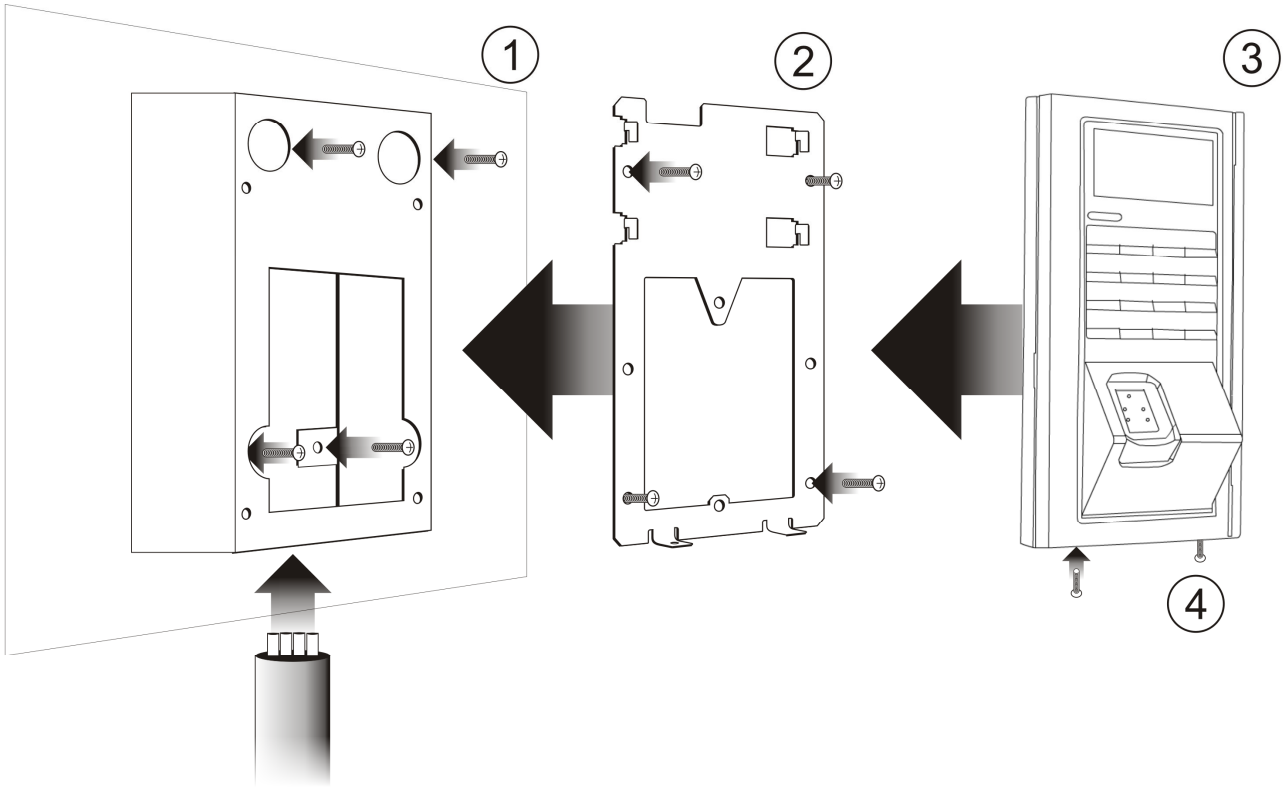


Figura 13 - Instalação com caixa metálica

1. Instalação da caixa metálica que serivrá de apoio ao suporte liso, aonde estarão presentes os cabos para conexão no dispositivo (alimentação, ethernet, conexões da fechadura e auxiliar, etc...):

   Na parte posterior da caixa existem 4 furos para os parafusos, utilizados para fixação da caixa na parede.

2. Instalação do suporte liso para encaixe do MCANet:

   A instalação do suporte liso consiste somente em seu encaixe e fixação dos parafusos nos quatro furos indicados na figura.

3. Encaixe do MCANet no suporte liso:

   Para colocar o MCANet no suporte liso, basta inseri-lo no mesmo e encaixa-lo empurrando-o para cima.

4. Fixação do MCANet no suporte liso:

   Existem na parte de baixo do MCANet, dois furos para inserção dos parafusos de fixação do duporte liso. Após o encaixe do MCANet, basta fixar os dois parafusos na parte de baixo do dispositivo.

   A seguir vemos como ficaria em perfil a fixação da caixa na parede.

   INSERIR FIGURA AQUI

7.1.3 Fixação utilizando caixa 2x4

A instalação do dispositivo com a utilização da caixa pode ser feita em 4 passos:

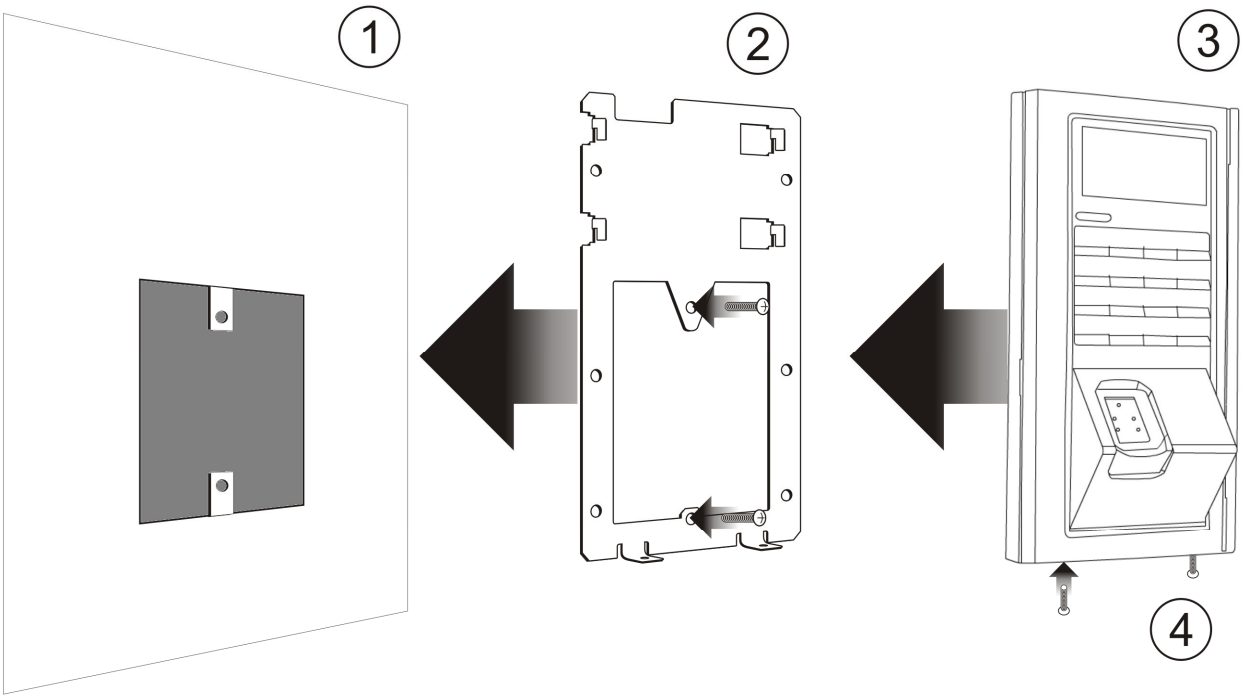


Figura 14 - Instalação com caixa metálica

1. Instalação do cabeamento estruturado com as conexões do dispositivo (alimentação, ethernet, conexões da fechadura e auxiliar, etc...).
2. Instalação do suporte liso para encaixe do MCANet:

   A instalação do suporte liso consiste somente em seu encaixe e fixação dos parafusos nos dois furos indicados na figura.
3. Encaixe do MCANet no suporte liso:

   Para colocar o MCANet no suporte liso, basta inseri-lo no mesmo e encaixa-lo empurrando-o para cima.
4. Fixação do MCANet no suporte liso:

   Existem na parte de baixo do MCANet, dois furos para inserção dos parafusos de fixação do duporte liso. Após o encaixe do MCANet, basta fixar os dois parafusos na parte de baixo do dispositivo.

   A seguir vemos como ficaria em perfil a fixação da caixa na parede.

   INSERIR FIGURA AQUI

7.1.4 Botão

7.1.5 Solenóides

7.1.6 Cabo Ethernet

7.2 Começando a utilizar o dispositivo

Para que o usuário possa começar a utilizar o dispositivo, a partir do momento em que este está ligado, pode acessá-lo com uma das senhas padrão cadastradas no mesmo.

O dispositivo vem configurado para acesso via teclado, e para começar a configuração e familiarização com o dispositivo, o usuário pode utilizar as seguintes senhas e IDs:

0001 – USER_01 – usuário para acesso ao local, senha: 12345678

0002 – USER_02 – técnico sem permissão de acesso, senha: 12345678

0003 – USER_03 – operador sem permissão de acesso, senha: 12345678

0004 – USER_04 – administrador com permissão acesso, senha: 12345678

RECOMENDA-SE QUE O USUÁRIO ALTERE AS SENHAS DE FÁBRICA ASSIM QUE A INSTALAÇÃO FOR CONCLUÍDA, A FIM DE NÃO PERMITIR QUE TERCEIROS TENHAM ACESSO AO SISTEMA SABENDO DAS CONFIGURAÇÕES PADRÃO.

Recomenda-se a leitura do manual antes de começar a utilizar o dispositivo efetivamente, para familiarizar-se com as funcionalidades e limitações do sistema.

Para entender como funcionam os periféricos do MCANet, o usuário deve consultar a seção 9 - Utilização. Lá estão listados todos os dispositivos que podem estar presentes no MCANet, bem como o modo de utilização de cada um.

8 Descrição do equipamento

Possuindo um formato moderno e prático o MCAnet possui um uma *display* de 128x64 pontos (LCD), teclado alfanumérico capacitivo para maior sensibilidade , 6 teclas de comando, Sensor biométrico para leitura de digitais, leitor de cartões de proximidade (MIFARE e RFId) e um leitor de código de barras.

Os dispositivos presentes podem variar, adequando-se á necessidade do usuário.

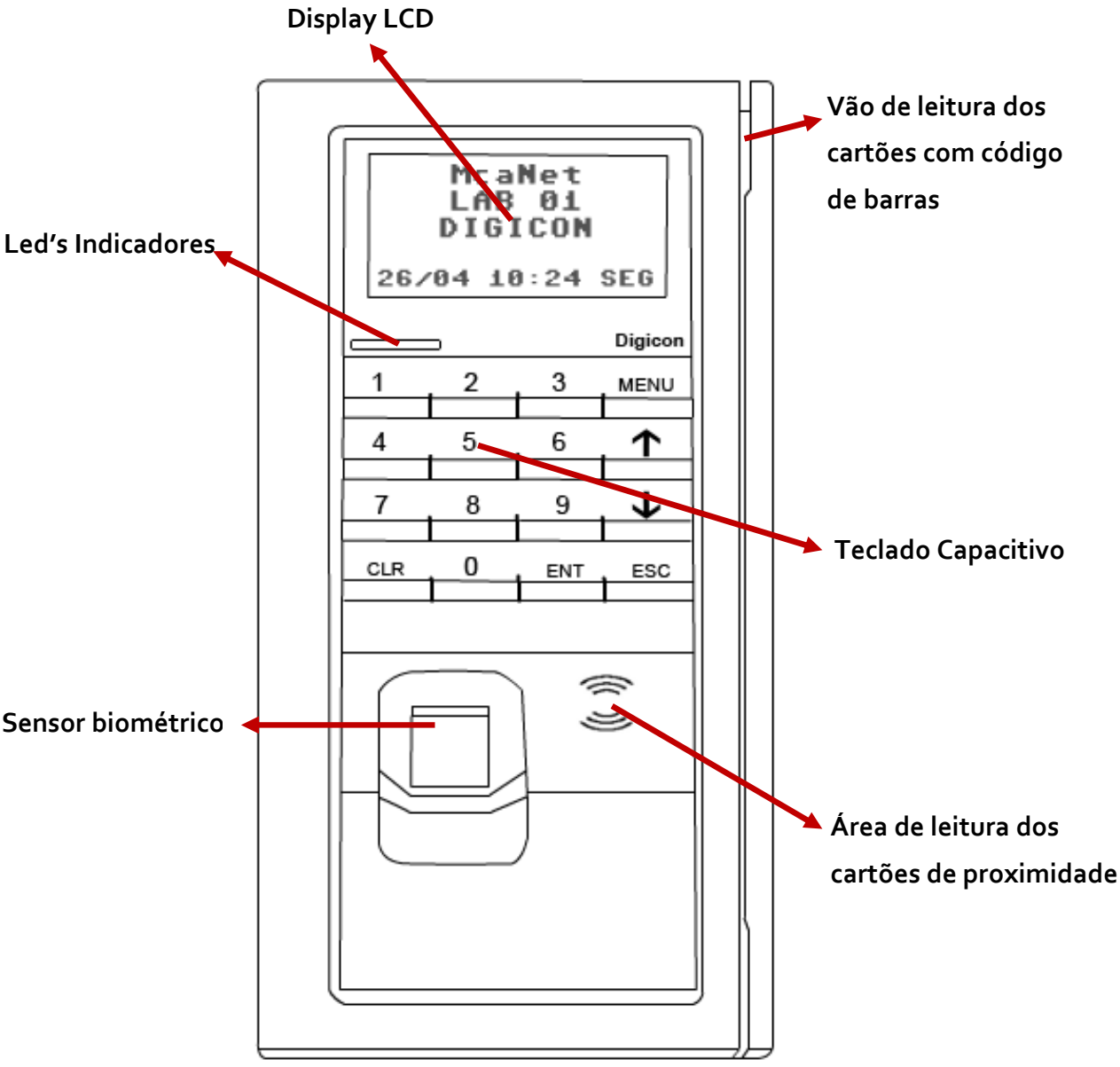


Figura 15 - Frente do dispositivo

9 Utilização

O MCANet possui um sistema de menus projetado para facilitar a configuração do dispositivo pelo usuário. Para cada perfil existem menus específicos, garantindo assim acesso de acordo com o perfil cadastrado para uma pessoa.

Em caso de perfis duplos (usuário + outro perfil), o menu mostrado será o do perfil com maior acesso ex.: Se um usuário for cadastrado como usuário + operador, o menu mostrado será o de operador.

A tela inicial do dispositivo, mostrada quando o dispositivo é ligado dá acesso tanto ao menu quanto ao local (porta), como mostrado abaixo:

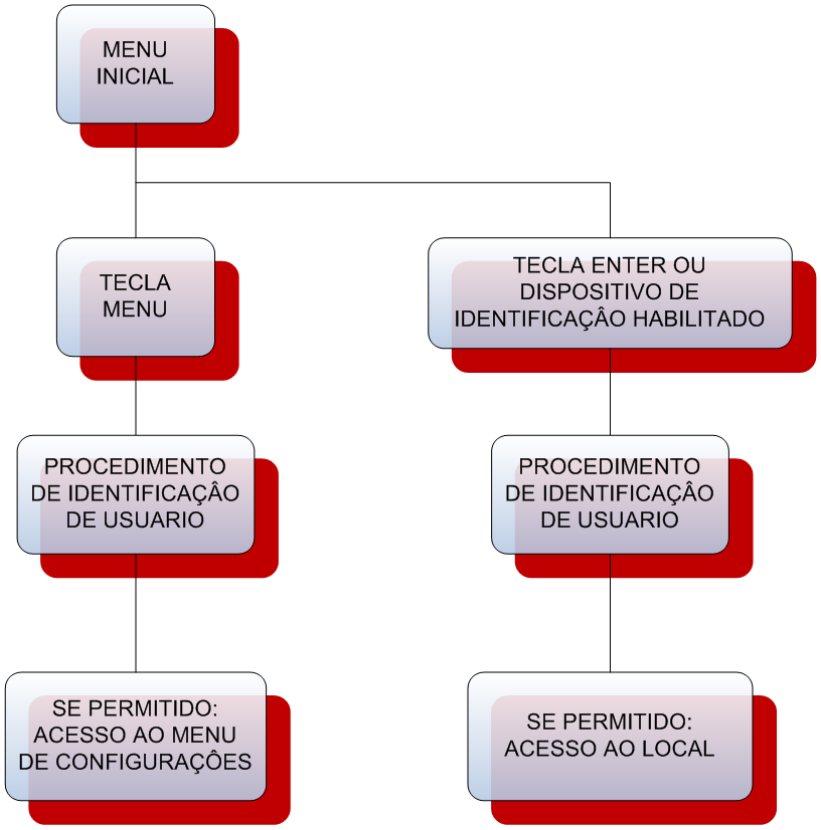

MENU INICIAL
TECLA MENU
TECLA ENTER OU DISPOSITIVO DE IDENTIFICAÇÂO HABILITADO
PROCEDIMENTO DE IDENTIFICAÇÂO DE USUARIO
PROCEDIMENTO DE IDENTIFICAÇÂO DE USUARIO
SE PERMITIDO: ACESSO AO MENU DE CONFIGURAÇÕES
SE PERMITIDO: ACESSO AO LOCAL

Figura 16 - Acesso aos menus e ao local

Quando for requisitado um acesso e o procedimento de identificação for finalizado, o usuário receberá na tela uma mensagem dizendo se foi ou não bem sucedido o procedimento de identificação.

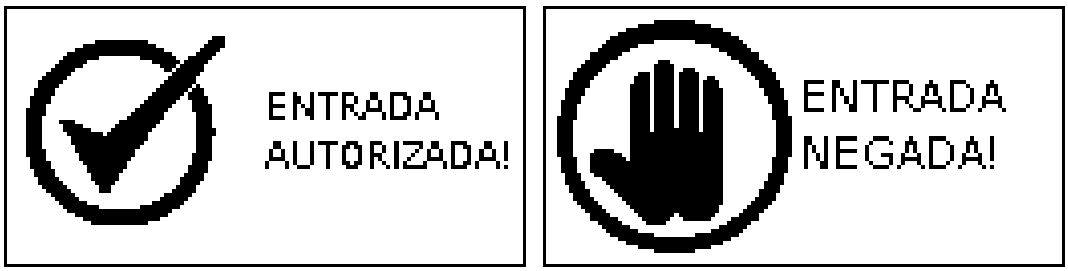


Figura 17 – ACESSO - Acesso permitido e acesso negado

Analogamente, quando o usuário requisitar a utilização do menu, será mostrada uma tela com o resultado da autenticação para a entrada no mesmo.

Figura 18 – MENU - Acesso permitido e acesso negado

9.1 Utilizando os dispositivos de autorização

Os vários dispositivos de autorização utilizados pelo Sistema de Acesso MCANet são listados nas seções a seguir, juntamente com seus modos de utilização. Para auxiliar o usuário o display irá sempre mostrar as instruções a serem seguidas em cada passo da autenticação ou cadastro de pessoal.

9.1.1 Sensor Biométrico de Digitais

O sensor biométrico de digitais é um dispositivo projetado para a identificação de pessoal através do escaneamento de suas digitais e comparação com dados previamente coletados durante o cadastro. Sistemas que utilizam este tipo de identificação são mais seguros e também mais cômodos, não necessitando que o usuário carregue qualquer outro tipo de identificação.

Para utilizar o sensor biométrico, basta posicionar o dedo desejado para cadastro ou identificação no mesmo após a luz se acender.

O fim do cadastro ou identificação chegará ao fim quando a luz se apagar, até que isto ocorra o usuário deve mantero dedo na posição de identificação indicada na figura.

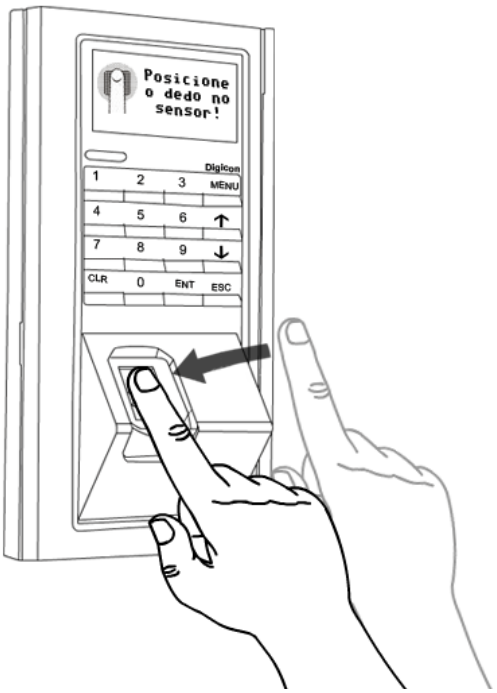


Figura 19 - Modo de utilização do sensor biométrico

9.1.2 Leitor de Código de Barras

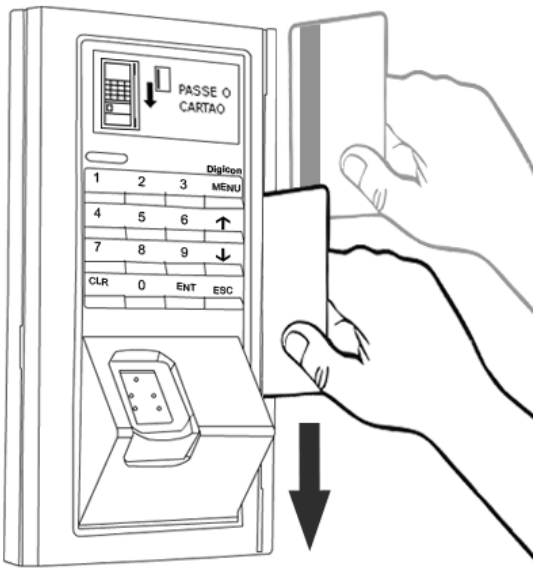


Figura 20 - Utilizando o leitor de código de Barras

A utilização do leitor de código de barras consiste simplesmente na passagem do cartão pelo vão de leitura até o fim, com a tarja de barras voltada para o lado do display.

É um procedimento rápido e simples e largamente utilizado no mercado atualmente.

9.1.3 Leitor de Cartão Mifare e RFID

Os leitores de cartão sem contato MIFARE e RFID são utilizados aproximando-se o cartão da área de leitura. Em ambos os casos o leitor fica na mesma posição.

Figura 21 - Utilização dos leitores sem contato

9.1.4 Teclado Capacitivo

O teclado do MCANet é um teclado capacitivo de alta sensibilidade, o que lhe possibilita um maior tempo de utilização bem como o pressionamento de teclas sem esforço por parte do usuário, simplesmente com a aproximação da ponta do dedo na tecla desejada.

Existem teclas de entrada de dados e teclas com funções especiais.

As teclas alfanuméricas são utilizadas para entrada de dados, quando requisitados pelas funções. Podem também servir como atalhos quando dentro do Menu, bastando pressionar o número equivalente a opção para acessá-la.

A tecla CLR serve para apagar dados em caso de erro na digitação. Nos campos numéricos ela apaga todo o campo, e nos campos alfanuméricos apaga somente o último caractere digitado.

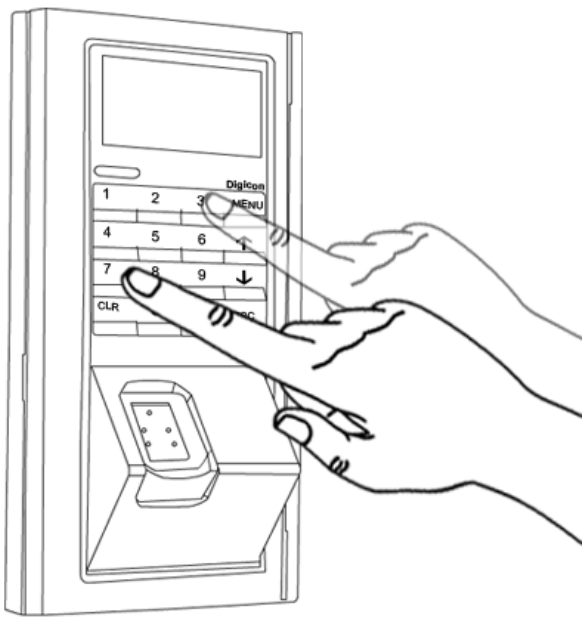


Figura 22 - Utilização do teclado Capacitivo

A tecla MENU, quando pressionada na tela inicial dá entrada ás opções de configuração.

As teclas ↑ (Para cima) e ↓ (para baixo) servem para navegação no menu e troca de campos, quando dentro das funções.

As teclas ENT e ESC, servem respectivamente para confirmar e cancelar uma operação. Porém quando dentro do menu, a tecla ENT seleciona uma opção, indo para a próxima tela do menu e a tecla ESC volta para a tela de menu anterior, ou no caso do menu principal, volta para a tela inicial.

É possível sair de uma função e voltar ao menu utilizando também a tecla ESC.

9.2 Entrada USB

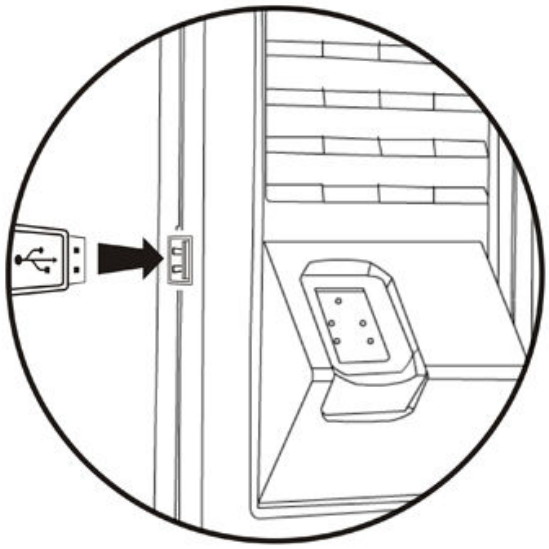


Figura 23 - Entrada USB

O dispositivo possui ainda uma entrada USB, utilizada para coleta de dados e atualização do firmware.

Sua utilização depende da funcionalidade desejada, portanto para entender mais, verificar as seções **BACKUP, ATUALIZAÇÂO DE FIRMWARE**, e **LISTAS.**

9.3 Navegando nos Menus

Para navegação nos menus, o usuário pode utilizar as teclas numéricas para acesso direto a uma função, ou utilizar as teclas ↑ (para cima), ou ↓ (para baixo), para mudar a função selecionada no momento e apertar ENT para acessar uma função ou submenu.

Para sair do Menu e voltar para a tela inicial, deve-se escolher a opção SAIR, existente em todas as telas de navegação. Quando dentro de uma função, não existirá esta opção, e deve-se pressionar a tecla ESC para retornar ao menu.

Quando acessado, será mostrado qual o perfil do usuário na barra de título:

Figura 24 - Tela do Menu

Nas seções a seguir serão listadas as árvores de menu para cada um dos usuários, e logo após uma lista com todas as funções disponíveis no dispositivo e suas finalidades.

9.4 Menu do Usuario

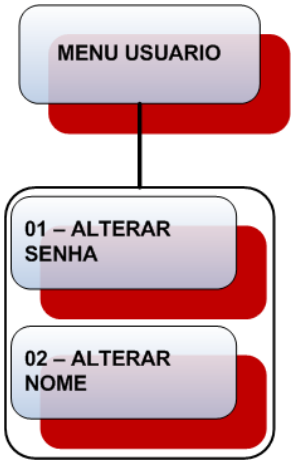


Figura 25 - Menu do Usuário

O usuário é o perfil mais simples de todos, tendo como permissões apenas o acesso ao local, a mudança da senha numérica e a mudança do nome no cadastro. Este perfil pode ser combinado com outros perfis, a fim de garantir ao mesmo tempo acesso e permissão para acesso aos menus avançados.

Uma pessoa cadastrada no dispositivo apenas como usuário visualizará em seu menu apenas as opções mostradas acima.

9.5 Menu do Técnico

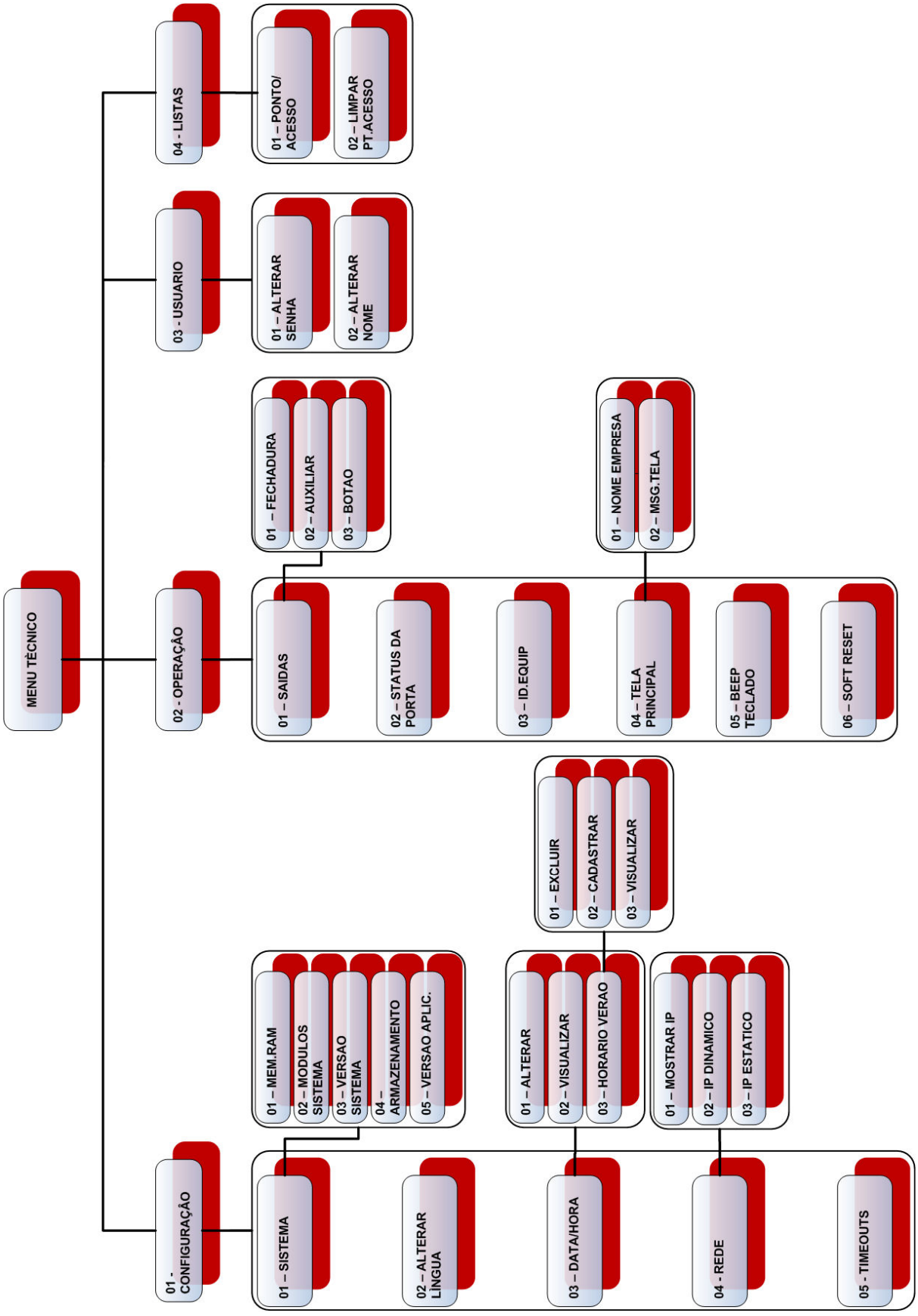


Figura 26 - Menu do Técnico

As Funções do Técnico consistem basicamente na coleta de dados (não relacionados á auditoria) e a configuração de funções básicas do dispositivo, como funções de auxílio á instalação (verficação de estado da entrada e configuração de acionamento de fechadura, saída auxiliar e botão interno de abertura da porta) e funções menores, como som do teclado e mensagens de tela.

9.6 Menu do Operador

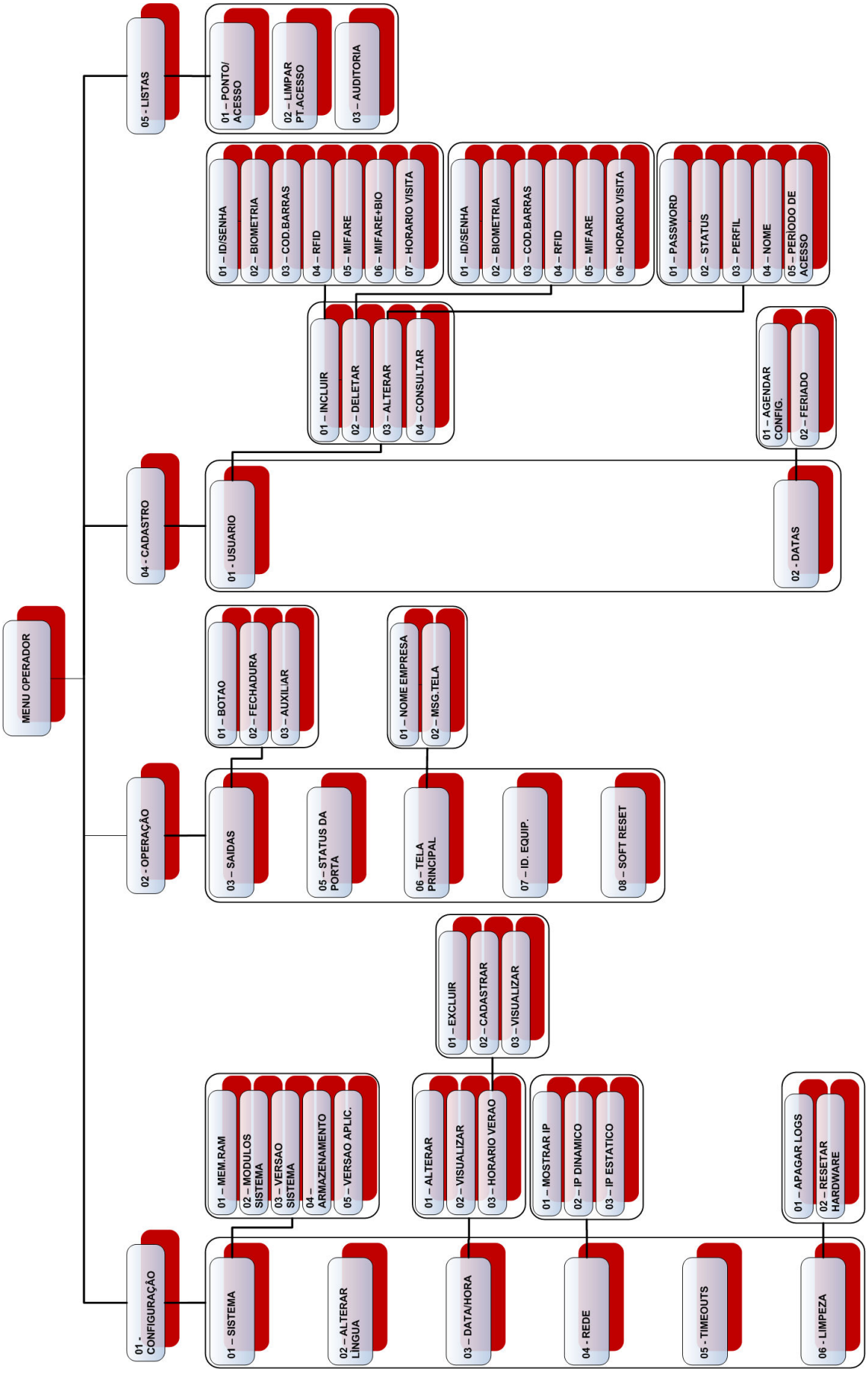


Figura 27 - Menu do Operador

O menu do Operador consiste basicamente das operações avançadas de manutenção. Não possui permissões relacionadas á auditoria, mudança dos dispositivos de autorização e do modo de operação.

Suas permissões são somente excedidas pelas funções do Administrador.

9.7 Menu do Administrador

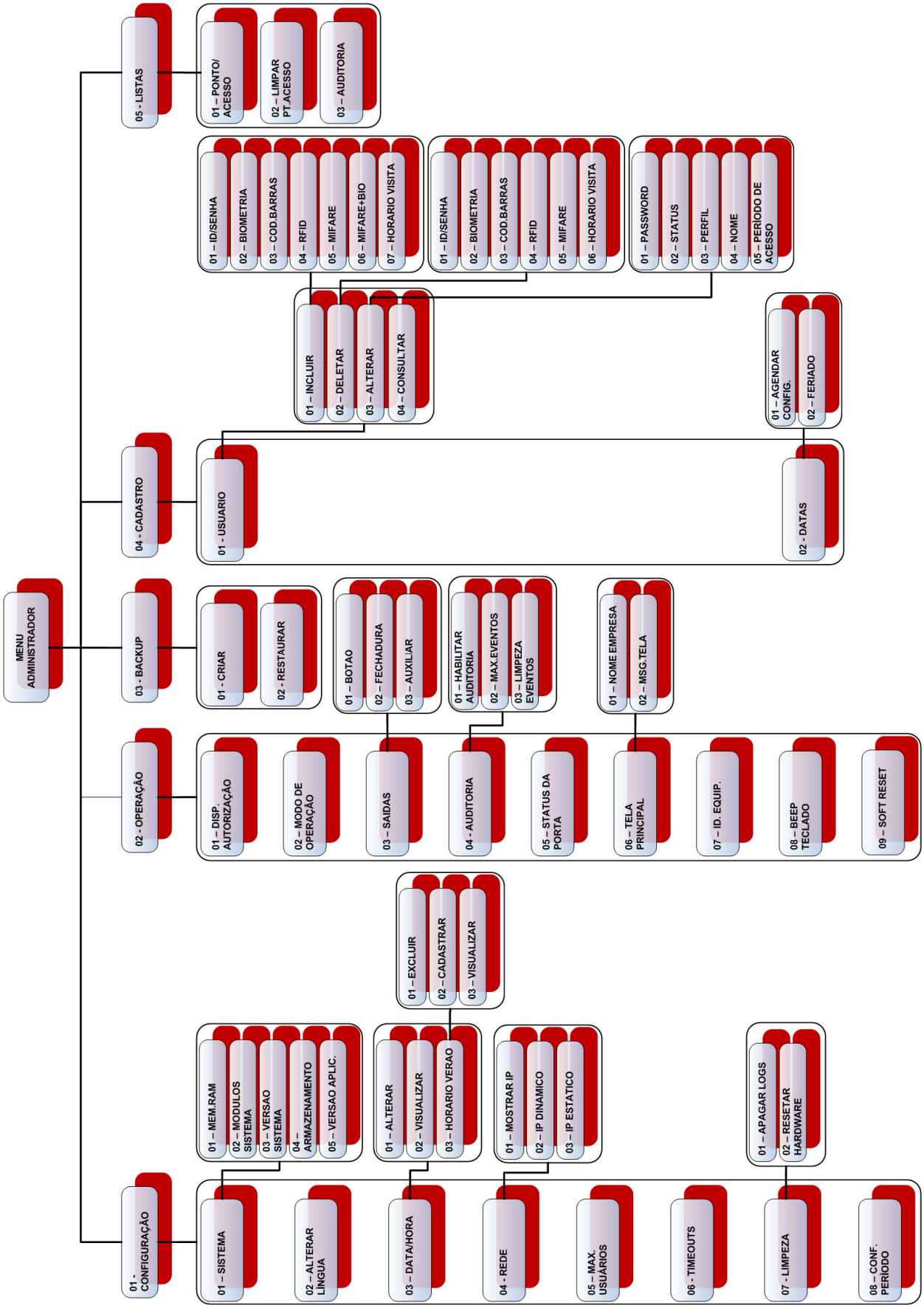


Figura 28 - Menu do Administrador

Todas as funções do sistema podem ser executadas pelo administrador. Este tipo de usuário pode alterar o modo de funcionamento do dispositivo e decidir como este deverá operar (ponto, acesso, dispositivos necessários á autorização, etc...), este usuário é o único que pode cadastrar outros administradores e alterar informações de todos os usuários.

9.8 Atualização de firmware do dispositivo

A atualização de firmware do dispositivo é feita de modo seguro e prático. Cada pacote de atualização é assinado pela DIGICON, ou seja, nenhum pacote não assinado pode ser instalado, garantindo que nenhum software mal-intencionado seja inserido no sistema.

Para atualizar, deve-se ter em mãos o pacote de atualização fornecido pela DIGICON, um dispositivo de armazenamento USB e uma conta com acesso ao menu avançado no dispositivo.

O pacote de atualização deve ser colocado em uma pasta chamada update na raiz do dispositivo de armazenamento. Caso esta não exista, o usuário deverá criá-la.

Estando com os arquivos na localidade correta, o usuário deve inserir a mídia de armazenamento na entrada USB do dispositivo (ver seção 9.2 - Entrada USB).

Após este passo, um usuário com perfil para entrada no menu avançado deve executar um soft reset no MCANet, (ver seção 9.11.9 - Soft Reset), e assim que o dispositivo se reiniciar será iniciado o procedimento de atualização do dispositivo. **O USUÀRIO NÃO DEVE REMOVER O DISPOSITIVO DE ARMAZENAMENTO DA ENTRADA USB DO MCANET DURANTE ESTE PROCEDIMENTO SOB PENA DE CORROMPER O FIRMWARE DO DISPOSITIVO.**

RECOMENDA-SE AO USUÁRIO FAZER O BACKUP ANTES DE EXECUTAR A ATUALIZAÇÂO DO DISPOSITIVO PARA NÃO PERDER SEUS DADOS DE ACESSO E CONFIGURAÇÕES JÁ CADASTRADAS.

Quando finalizada a atualização a aplicação será iniciada novamente. Após esta ocorrência o usuário poderá remover a mídia da entrada USB.

9.9 Descrição dos Menus e Funções

Abaixo listaremos todas as funções disponíveis dentro do dispositivo. Para Informações sobre a disponibilidade de cada uma de acordo com um determinado perfil, procurar a seção 9 – Utilização.

9.10 Menu Configuração

Este Menu guarda todas as funções necessárias para alteração e visualização das configurações básicas do sistema. Podem-se consultar aqui informações como memória, versão do sistema e aplicação, alterar língua e data do sistema e outras configurações. Utilizado primariamente par obter informações necessárias à manutenção do dispositivo.

9.10.1 Menu Sistema

O menu de sistema serve para visualização de informações relativas ao hardware e ao firmware correntes no dispositivo.

9.10.1.1 Memória RAM

Mostra os dados de memória RAM do sistema (memória livre e utilizada), em quantidade de bytes e em porcentagem do total disponível no sistema.

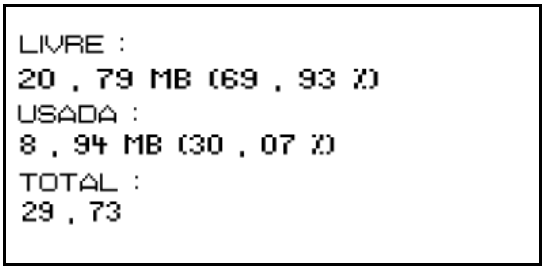


Figura 29 - Consulta da memória RAM

9.10.1.2 Módulos de Sistema

Mostra a versão dos módulos utilizados no sistema. Serve para o acompanhamento das funcionalidades, mostrando quais módulos estão instalados e suas versões.

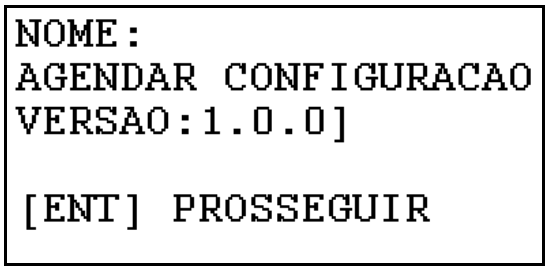


Figura 30 - Consulta dos módulos do sistema

O usuário pode navegar nesta tela, apertando a tecla ENT para passar para o próximo módulo. Se necessário pode também abortar a visualização pressionando a tecla ESC.

9.10.1.3 Versão do Sistema

Mostra a versão do sistema operacional utilizado.

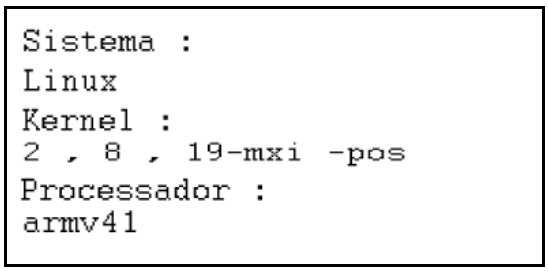


Figura 31 - Versão do sistema Operacional

9.10.1.4 *Armazenamento*

Mostra a quantidade de memória disponível.

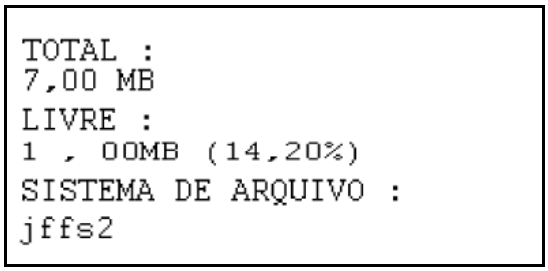


Figura 32 - Consulta de Armazenamento

9.10.1.5 *Versão Aplicativo*

Mostra a versão do aplicativo instalado.

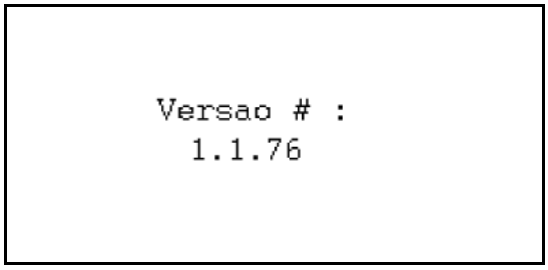


Figura 33 - Versão do aplicativo

9.10.2 Alterar língua

Altera a linguagem das mensagens do MCANet. Na versão atual são suportadas as linguagens PORTUGUES e INGLES.

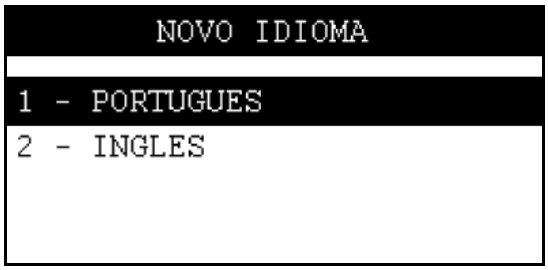


Figura 34 - Seleção de linguagem

Após a escolha da linguagem para alteração, será mostrada uma tela para confirmação da alteração:

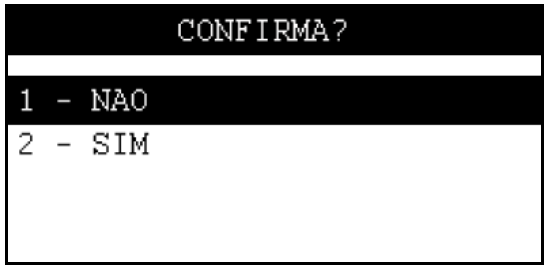


Figura 35 - Confirmação de exclusão de horário de verão

Confirmando a operação, será mostrada uma tela indicando sucesso ou falha na alteração, e depois o dispositivo será reiniciado para aplicar as novas configurações.

9.10.3 Menu Data/Hora

O menu de DATA/HORA mostra as configurações relativas ao horário do sistema, como o data e hora atuais e a configuração para funcionamento em horário de verão.

9.10.3.1 Alterar Data/Hora

Ao selecionar a função, será mostrada uma tela ao usuário para que este esolha a data do sistema.

O primeiro campo deve conter a data para alteração e o segundo deve conter a hora. Ao finalizar o preenchimento dos campos o usuário deve confirmar a alteração apertando a tecla ENT ou pode também cancelar a operação pressionando a tecla ESC.

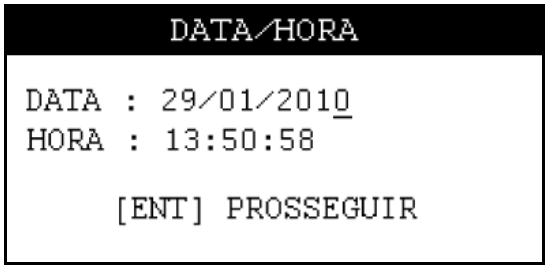


Figura 36 - Tela de alteração de data/hora

Após o preenchimento dos campos, caso a data e hora informada sejam válidas, será mostrada uma tela para confirmação da alteração:

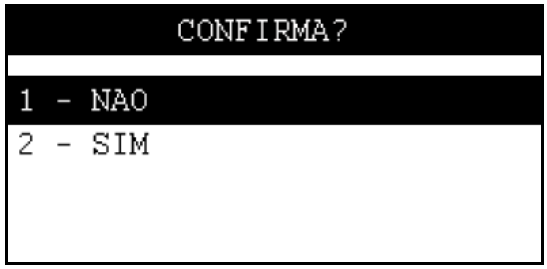


Figura 37 - Confirmação de exclusão de horário de verão

Ao finalizar a operação, será mostrada uma tela de com o resultado da mesma.

9.10.3.2 Visualizar Data/Hora

Esta função mostra ao usuário a data e hora correntes do sistema.

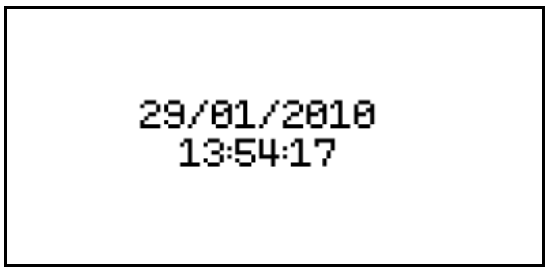


Figura 38 - Visualização de data/hora

9.10.3.3 Menu Horário de Verão

Dentro deste menu se encontras as configurações relativas ao horário de verão. Existe somente um cadastro para período de horário de verão, sendo que em caso de cadastro de um novo período o anterior será sobreposto. A exclusão do período de horário de verão irá apagar o período cadastrado, caso haja algum.

A ativação do horário de verão implica somente no seu cadastro, pois a ativação do mesmo se dará automaticamente após a data de início.

9.10.3.3.1 Excluir Horário de Verão

A exclusão do horário de verão pedirá apenas a confirmação da operação. Caso seja mesmo o intento do usuário de desligar o horário de verão e apagar o período cadastrado, basta que este selecione SIM.

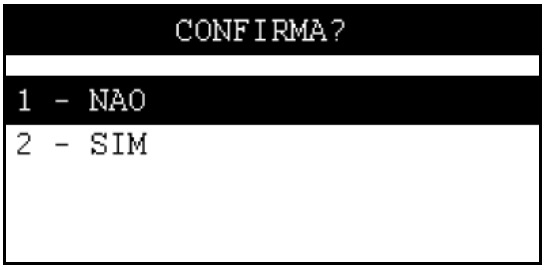


Figura 39 - Confirmação de exclusão de horário de verão

9.10.3.3.2 Cadastrar Horário de Verão

Para o cadastro de um período para o horário de verão, serão apresentadas duas telas, uma para escolha da data de início e outra para a data de fim. Após este cadastro, o horário de verão será automaticamente acionado com o passar da data cadastrada de início e voltará ao normal após a data cadastrada para o fim.

Para ir de uma tela para outra o usuário precisa preencher os dois campos, pressionando ENT após preencher cada campo.

Durante o cadastro da data o usuário poderá cancelar a operação a qualquer momento apertando a tecla ESC.

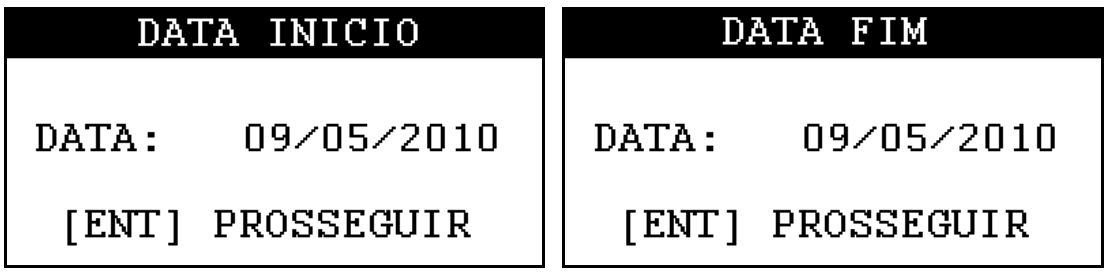


Figura 40 - Cadastro de horário de verão

Após o término da operação será mostrada uma tela com o resultado da operação.

9.10.3.3.3 *Visualizar Horário de Verão*

Nesta opção será mostrada a configuração atual do horário de verão (se está ativo e também mostrando o horário cadastrado atualmente, caso não haja nenhum horário cadastrado, todos os campos estarão preenchidos com zero).

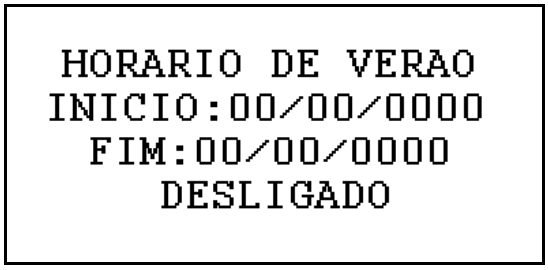


Figura 41 - Visualização de horário de verão

9.10.4 Menu REDE

Neste menu podem ser configurados os parâmetros de acesso á rede do dispositivo.

9.10.4.1 *Mostrar IP*

Esta função permite ao usuário visualizar o IP do sispotivo, caso este estaja conectado á rede.

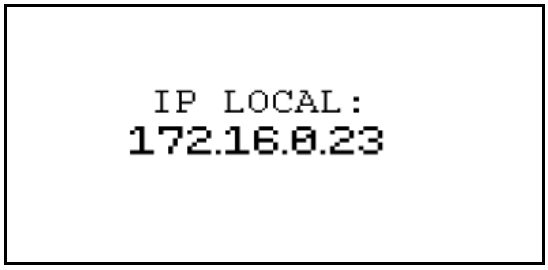


Figura 42 - Visualização de endereço de rede do dispositivo

9.10.4.2 *IP Dinâmico*

Nesta função o usuário pode configurar o dispositivo para acesso á rede com IP dinâmico. Será pedida apenas a confirmação do usuário para a mudança de configuração.

Esta configuração será válida apenas para redes que suportam endereços IP atribuídos por DHCP. Caso não haja um servidor DHCP, o dispositivo não será capaz de resolver seu IP.

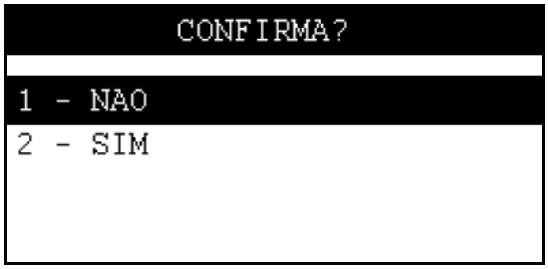


Figura 43 – Configuração de acesso á rede com IP Dinâmico

Após a mudança, será exibida uma tela como resultado da operação.

9.10.4.3 *IP Estático*

Nesta função o usuário pode configurar o dispositivo para acesso á rede com IP estático, fornecendo o IP, o gateway e a máscara de rede.

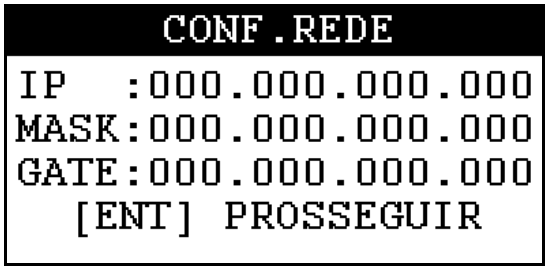


Figura 44 – Configuração de acesso á rede com IP Estático

Cada um dos parâmetros deve ser preenchido, e quando finalizado o preenchimento o usuário deve confirmar apertando a tecla ENT. Será pedida então uma confirmação para a alteração da configuração.

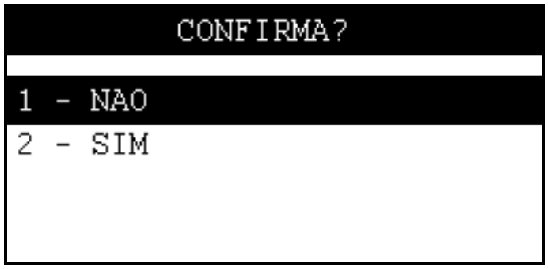


Figura 45 – Confirmação de acesso á rede com IP Estático

Após a seleção, será mostrada uma tela com o resultado da operação.

9.10.5 Max. Usuários

O número de usuários que podem ser cadastrados no MCANet pode ser configurado a partir desta função.

O usuário deve ter em vista que tendo cadastros prévios, **NÃO SERÁ POSSÍVEL ALTERAR O NÚMERO DE USUÁRIOS PARA UM NÚMERO MENOR DO QUE O NÚMERO DE USUÁRIOS JÁ CADASTRADOS.**

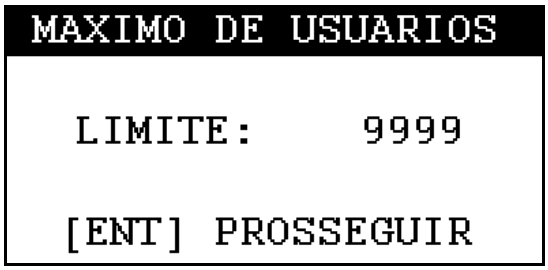


Figura 46 – Configuração de número de usuários

9.10.6 Timeouts

Os tempos de espera do dispositivo para cada situação podem ser configurados. Nesta função podem ser alterados:

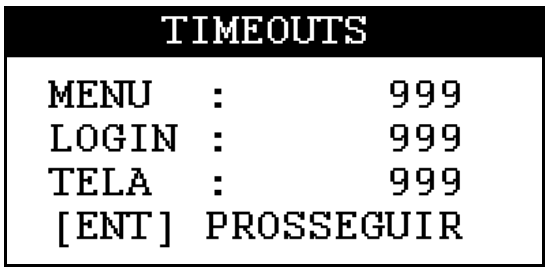


Figura 47 – Configuração de Timeouts

Tempo de espera do Menu – Quando o menu é acessado, caso o usuário passe um tempo maior do que o tempo de espera sem acessar nenhuma das opções de menu, este volta para a tela inicial do dispositivo após esperar a quantidade de tempo indicada neste campo.

Tempo de espera para Login – Cada etapa de verificação terá o tempo de espera indicado nesta função. Ex: Para uma situação em que o tempo de login é de 10 segundos, e em que temos um processo de identificação que executa verificação de teclado e depois biometria, serão esperados 10 segundos para digitação de senha e 10 segundos para inserção de biometria.

Tempo de espera de Tela – A tela inicial possui uma opção de descanso, ou seja após a espera do tempo indicado neste campo o display e os dispositivos de identificação serão desativados para economia de energia.

Quando cadastrado o valor máximo de 999 para um tempo de espera, este será considerado infinito, i.e. o dispositivo nunca sairá do estado em que se encontra por exceder o tempo de espera.

Todos os tempos nesta função são medidos em segundos.

Após a inserção dos valores nos três campos, o usuário deve pressionar ENT para finalizar a operação, ou em qualquer momento ele pode pressionar ESC para cancelar a operação.

Após a passagem dos parâmetros o usuário deve confirmar a alteração da configuração.

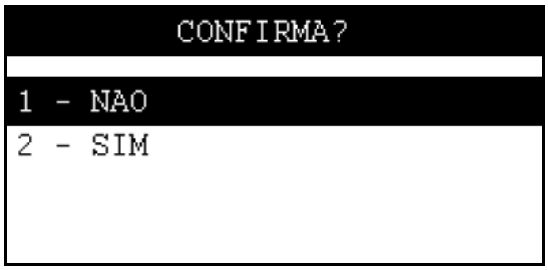


Figura 48 – Confirmação de alteração de timeouts

Após a seleção, será mostrada uma tela com o resultado da operação.

9.10.7 Menu Limpeza

Este menu contém as funções de limpeza de memória do dispositivo.

9.10.7.1 Apagar Logs

Apaga os logs de depuração do dispositivo.

Quando selecionada, esta opção apenas pede a confirmação do usuário.

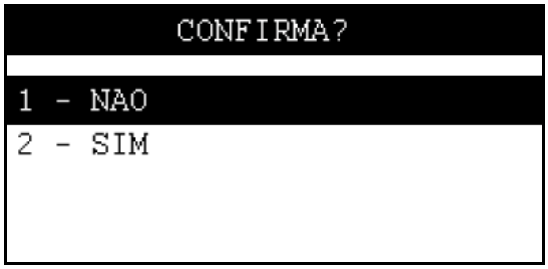


Figura 49 – Limpeza dos Logs

Quando finalizada a operação, uma tela será mostrada com o resultado.

9.10.7.2 Resetar Hardware

Esta função retorna o dispositivo às configurações de fábrica, **APAGANDO TODAS AS INFORMAÇÕES JÁ REGISTRADAS E RESTAURANDO AS CONFIGURAÇÕES QUE O DISPOSITIVO TINHA QUANDO SAIU DA CAIXA PELA PRIMEIRA VEZ.**

Será requisitada a confirmação do usuário para a execução desta função. É de extrema importância que o usuário não se envolva com o dispositivo neste momento, em hipótese alguma deve desligar o dispositivo, **SOB PENA DE CORROMPER DADOS E DANIFICAR ARQUIVOS DA APLICAÇÃO DO DISPOSITIVO**.

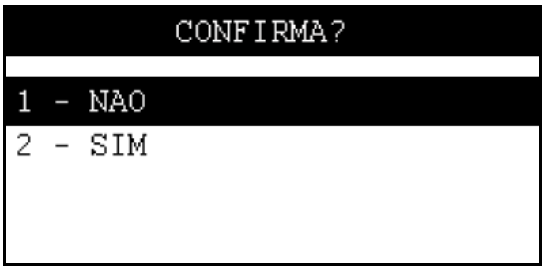


Figura 50 – Confirmação de Resetar Hardware

Enquanto o dispositivo estiver executando a operação de reset, será mostrada uma tela indicando que o usuário deve esperar.

Após o término da operação será mostrada uma tela com o resultado, e depois o dispositivo se reiniciará para aplicar as novas configurações.

9.10.8 Conf. Período

Esta opção configura o período de acesso para usuários cadastrados a partir de sua alteração, ou seja, novos usuários cadastrados terão como período de acesso em sua criação o período especificado por esta função. Esta função não altera o período de acesso de usuários previamente cadastrados.

Primeiramente será questionado ao usuário quais dias da semana serão liberados.

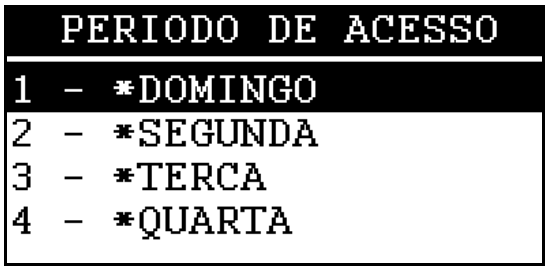


Figura 51 – Configuração de período – dias da semana

Para selecionar um dia, basta apertar ENT ou a numeração ao lado do dia selecionado. Dias selecionados serão marcados por um '*' ao lado, e podem ser desmarcados, bastando seleciona-los novamente.

O próximo passo é escolher o horário de acesso, sendo a tela a seguir a tela para escolha da hora de início do período.

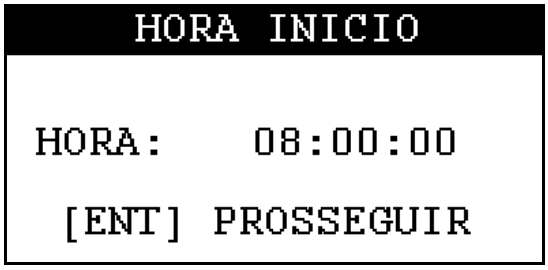


Figura 52 – Configuração de período – hora início

Nesta tela o usuário deve selecionara a hora de início, e após o término do preenchimento deve pressionar a tecla ENT.

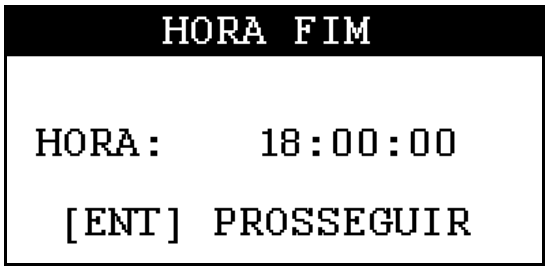


Figura 53 – Configuração de período – hora fim

Na próxima tela o usuário deve escolher a hora de fim do período, e após o término do preenchimento deve presionar a tecla ENT.

A próxima tela é para escolha da data de fim do período (após esta data, um usuário cadastrado segundo estas configurações não terá mais acesso, a não ser que o período de acesso do mesmo especificamente seja alterado).

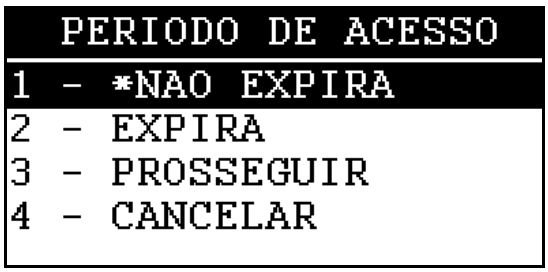


Figura 54 – Configuração de período – expiração

Nesta tela a opção desejada estará marcada.

A opção NÃO EXPIRA faz com que o usuário tenha permissão para acesso (dentro dos dias e horas cadastrados) sem data para expiração de acesso, e finaliza a operação.

A opção EXPIRA segue para uma tela, onde o usuário deve escolher um prazo para expiração do tempo de acesso em semanas, ou seja, cada usuário cadastrado terá acesso da data atual de seu cadastro até o fim do número de semanas informado.

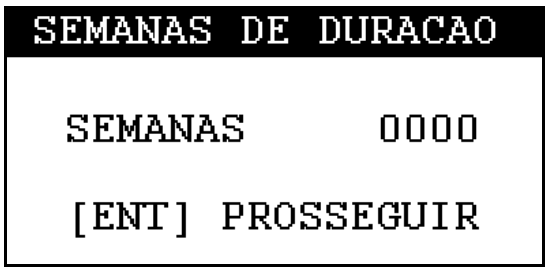


Figura 55 – Configuração de período – Tempo para expiração

Após a escolha do período para o fim a operação será finalizada.

A opção PROSSEGUIR executa a opção selecionada pelo usuário.

A opção CANCELAR sai da função sem salvar as alterações.

Após o fim da operação será exibida uma tela com o resultado final da operação.

9.10.9 Chave MIFARE

Esta função serve para a escolha da senha utilizada para a geração das chaves do cartão MIFARE. O usuário deve ficar atento ao utilizar esta opção pois **A ALTERAÇÂO DA CHAVE DO MIFARE IRÁ INUTILIZAR OS CARTÕES DE MIFARE COM BIOMETRIA PREVIAMENTE CADASTRADOS, A NÃO SER QUE O USUARIO VOLTE A UTILIZAR A CHAVE VIGENTE NO MOMENTO EM QUE OS MESMOS FORAM CADASTRADOS.**

OS CARTÕES QUE PODEM SER CADASTRADOS DEVEM TER OU CHAVES DE FÁBRICA OU CHAVES GERADAS PELO PRÓPRIO DISPOSITIVO COM A CHAVE ATUAL.

Esta função possui uma única tela, aonde o usuário deverá inserir uma chave de 15 dígitos, utilizada na criação das chaves dos setores.

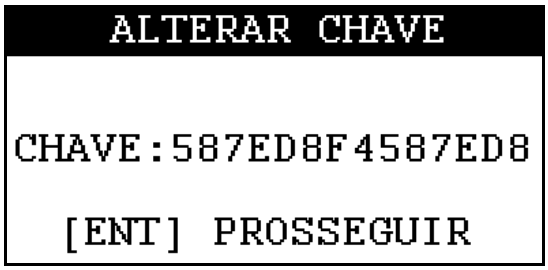


Figura 56 – Entrada de chave dos cartões MIFARE

Para finalizar, o usuário deve confirmar a operação:

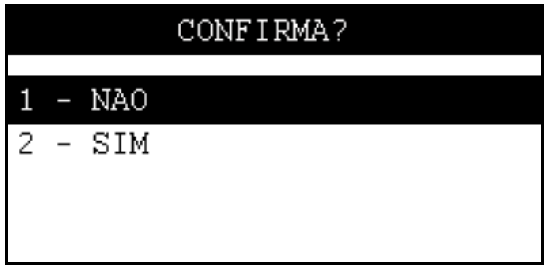


Figura 57 – Tela de confirmação da alteração de chave do MIFARE

Após o fim da operação será mostrada uma tela com o resultado da operação.

9.11 Menu Operação

Este menu guarda as opções relativas a configurações de operação do dispositivo, como dispositivos de autorização ativos, configuração de fechaduras e saídas, etc...

9.11.1 Dispositivos de Autorização

Controla os dispositivos que serão utilizados para autenticar os usuários. Podem ser utilizadas várias combinações de dispositivos, e cada um deles será uma etapa na identificação do usuário.

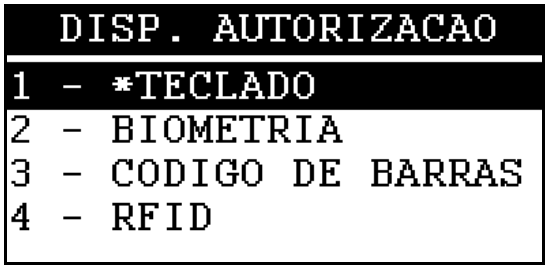


Figura 58 – Seleção de dispositivos de autorização

Ao selecionar uma das opções de dispositivos, o mesmo será marcado e pode ser desmarcado mediante nova seleção. Existe um caso especial de identificação que é o MIFARE+BIOMETRIA, que quando selecionado irá desmarcar as opções de MIFARE e BIOMETRIA. O modo de utilização e os detalhes deste tipo de identificação serão explicitados na seção de cadastro de MIFARE+BIOMETRIA.

Para finalizar o procedimento de seleção, o usuário deve selecionar a opção FINALIZAR, ou se mudar de idéia quanto á operação pode sempre cancelar a mesma, pressionando a tecla ESC ou a opção CANCELAR.

Para aplicar as configurações, o usuário deverá confirmar.

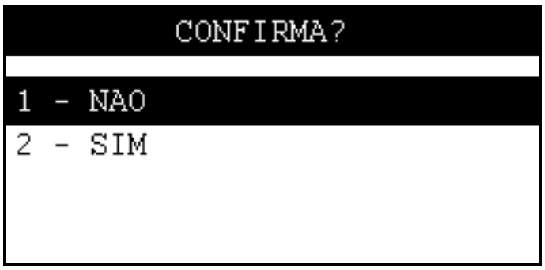


Figura 59 – Tela de confirmação da alteração de dispositivos de operação

Após o fim da operação, será mostrada uma tela com o resultado da operação e o dispositivo será reiniciado para aplicar a nova configuração.

9.11.2 Modo de Operação

Seleciona o modo de funcionamento do dispositivo. O MCANet pode ser configurado de três modos diferentes:

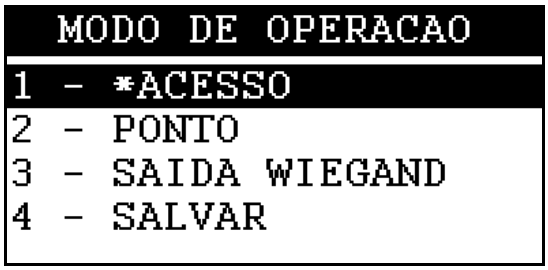


Figura 6o – Tela de seleção de modo de acesso

- MODO ACESSO – Quando habilitado, este modo acionará a saída que libera o acesso do usuário quando a autorização for bem sucedida. São guardados em base de dados os dados de acesso de cada usuário.

- MODO PONTO – Guarda em base de dados informações sobre o horário de ponto do usuário em questão. Estas informações podem ser recolhidas por um usuário avançado no menu LISTAS-PONTO/ACESSO

- MODO SAÍDA WIEGAND – Quando for bem-sucedida a autorização, neste modo o dispositivo enviará pela saída WIEGAND as informações do usuário. Esta saída serve para permitir a integração do MCANet com sistemas que possuam este padrão.

Cada um dos modos de acesso pode ser combinado, e podemos ter então um dispositivo que sirva como autorizador de acesso, marcador de ponto e que utilize um identificador externo capaz de receber sinais via WIEGAND.

Um modo de acesso selecionado será marcado, podendo ser desmarcado se selecionado novamente.

Para finalizar o usuário deverá confirmar a operação.

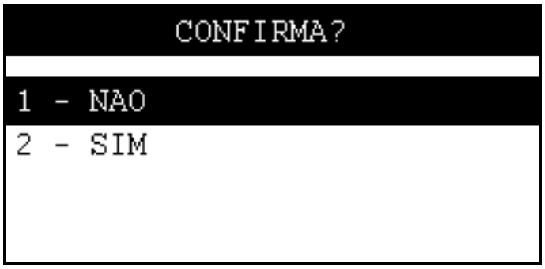


Figura 61 – Tela de confirmação da alteração de modo de operação

Após a escolha do modo desejado, o usuário pode aplicar as configuração utilizando a opção SALVAR, ou cancelar utilizando a tecla ESC ou a opção CANCELAR.

9.11.3 Menu Saídas

Este menu contém as opções das saídas que serão acionadas quando as identificações de usuário forem bem ou mal sucedidas.

9.11.3.1 Botão

Este opção existe para abertura a partir do interior da localidade que está sendo monitorada, isto é, no interior da sala ou local sendo guardada pelo MCANet poderá existir um botão para que a porta seja aberta sem a necessidade de identificação por parte de um usuário no exterior da localidade.

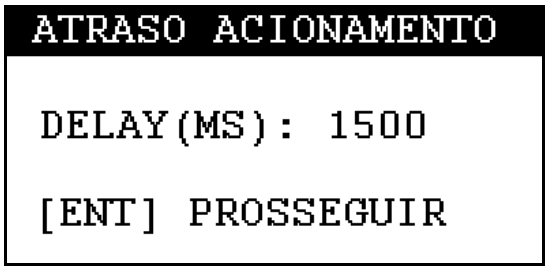


Figura 62 – Tela de configuração do botão

A única opção a ser configurada é o tempo durante o qual o botão precisa ficar apertado até que o acesso seja garantido. Esta opção serve para evitar que ruído na conexão do botão acidentalmente abra a porta, garantindo que a abertura seja feita somente com o consentimento de um usuário no interior do local.

Após a seleção do tempo de delay (tempo decorrido entre o apertar do botão e a liberação do acesso), para finalizar a operação, o usuário deve confirmar a operação ou teclar ESC para cancelar.

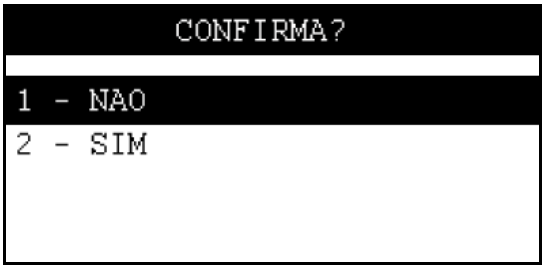


Figura 63 – Tela de confirmação da alteração de acionamento de botao

Ao confirmar a mudança, o dispositivo irá se reiniciar para completar a operação.

9.11.3.2 Fechadura

Configura qual saída será utilizada como fechadura, qual o tempo de acionamento e qual o estado padrão da saída.

Esta configurção permite que o usuário não se atenha a um único modelo de fechadura, por exemplo, permitindo que o dispositivo se adapte ao sistema.

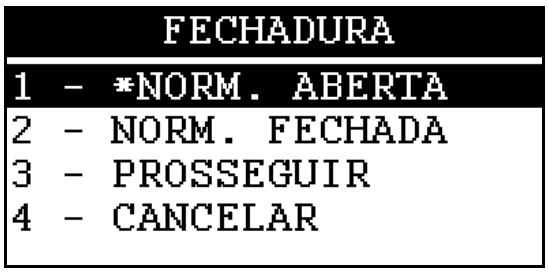


Figura 64 – Tela de escolha do estado da fechadura

A primeira tela de configuração é a escolha do estado da saída, e pode assumir duas configurações:

- NORMALMENTE ABERTA – O contato sempre fica em aberto, a não ser quando for requisitado seu acionamento, ou seja, durante o acionamento irá para o estado de tensão alta e depois retornará ao estado de baixa tensão.

- NORMALMENTE FECHADA - O contato sempre fica fechado, a não ser quando for requisitado seu acionamento, ou seja, durante o acionamento irá para o estado de tensão baixa e depois retornará ao estado de baixa alta.

Para continuar o usuário deve escolher a opção 3 ou a opção 4 para sair da função.

A segunda tela serve para a escolha de qual das saídas será acionada quando o acesso for permitido.

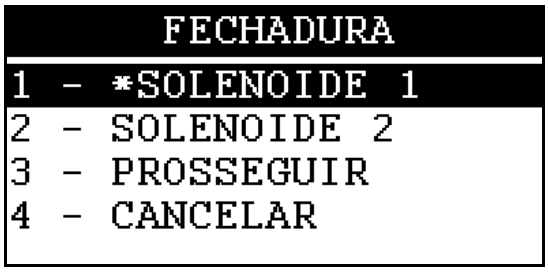


Figura 65 – Tela de escolha do solenóide da fechadura

Existem dois solenóides que podem ser utilziados no dispositivo, sendo que quando um é selecionado para se o solenóide da fechadura, o outro será automaticamente selecionado para ser a saída auxiliar (vide seção AUXILIAR). O mesmo vale para a configuração da saída Auxiliar.

Selecionando o solenóide desejado o usuário pode passar á próxima tela selecionando a opção PROSSEGUIR ou para a operação com a opção CANCELAR.

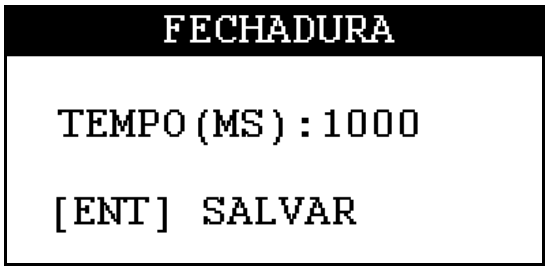


Figura 66 – Tempo de acionamento da fechadura

O tempo configurado nesta tela é o tempo em que o solenóide ficará acionado quando for solicitado. Este tempo é configurável devido aos vários modelos diferentes de acionamentos (fechaduras, etc...) existentes que podem ser utilizados.

Este tempo é configurado em millisegundos, e para finalizar sua configuração o usuário deve pressionar a tecla ENT ou ESC para cancelar toda a operação.

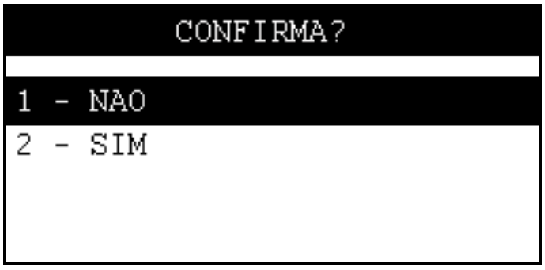


Figura 67 – Tela de confirmação da configuração da fechadura

Ao fim da configuração o usuário deve confirmar se deseja gravar os novos parâmetros.

9.11.3.3 Auxiliar

Configura a utilização de uma saída auxiliar a ser acionada quando o usuário não for autenticado com sucesso, acionando um alarme ou no caso de utilização doméstica uma campainha por exemplo.

A primeira tela configura a utilização ou não desta entrada.

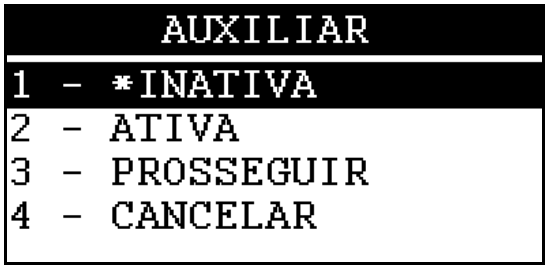


Figura 68 – Tela de configuração da saída auxiliar

Selecionando INATIVA, o dispositivo não acionará a saída auxiliar, e selecionando ATIVA o a mesma será acionada em caso de falha na autenticação de um usuário.

A próxima tela de configuração é a escolha do estado da saída:

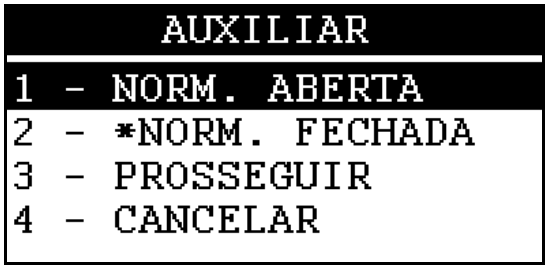


Figura 69 – Tela de escolha do estado da saída auxiliar

Esta pode assumir duas configurações:

- NORMALMENTE ABERTA – O contato sempre fica em aberto, a não ser quando for requisitado seu acionamento, ou seja, durante o acionamento irá para o estado de tensão alta e depois retornará ao estado de baixa tensão.

- NORMALMENTE FECHADA - O contato sempre fica fechado, a não ser quando for requisitado seu acionamento, ou seja, durante o acionamento irá para o estado de tensão baixa e depois retornará ao estado de baixa alta.

Para continuar o usuário deve escolher a opção 3 ou a opção 4 para sair da função.

A próxima configuração é a configuração do tempo de acionamento da saída auxiliar:

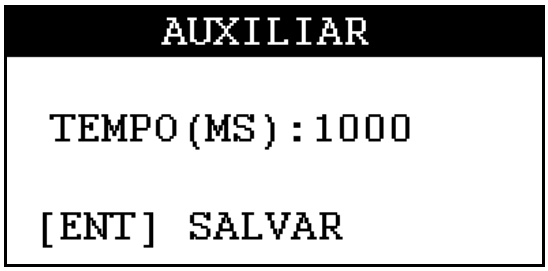


Figura 70 – Tela de configuração do tempo de acionamento da saída auxiliar

O tempo configurado nesta tela é o tempo em que o solenóide ficará acionado quando for solicitado. Este tempo é configurável devido aos vários modelos diferentes de acionamentos (fechaduras, etc...) existentes que podem ser utilizados.

Este tempo é configurado em millisegundos, e para finalizar sua configuração o usuário deve pressionar a tecla ENT ou ESC para cancelar toda a operação.

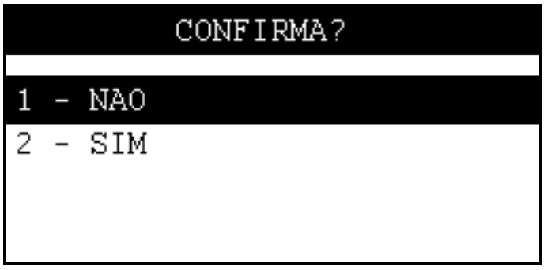


Figura 71 – Tela de confirmação da configuração da auxiliar

Finalimente o usuário deverá confirmar se deseja ou não salvar as configurações selecionadas.

9.11.4 Menu Auditoria

O menu de auditoria contém funções para configuração da monitoração de atividades do sistema. Por este menu, o usuário pode habilitar ou não o registro de eventos de auditoria, a quantidade de eventos que irá guardar na memória e limpar eventos já salvos.

Eventos de auditoria são informações salvas no momento em que uma operação a feita, a fim de esclarecer os motivos do usuário que realizou a operação. O armazenamento deste tipo de informação permite que um administrador do sistema, em casos aonde se suspeita de falha humana na operação do dispositivo (mal-intencionada ou não), seja capaz de traçar os passos realizados pelo usuário em questão a fim de descobrir o que o mesmo fez e quais foram suas intenções.

Um evento de auditoria, caso a mesma esteja habilitada, é armazenado toda vez que um usuário executa uma operação, de acesso (permitido ou negado) ou alteração de configuração (indica quais funções o usuário acessou, tendo sido bem-sucedida ou não).

9.11.4.1 Habilitar Auditoria

Esta função pode ligar ou desligar o armazenamento de eventos de auditoria do sistema.

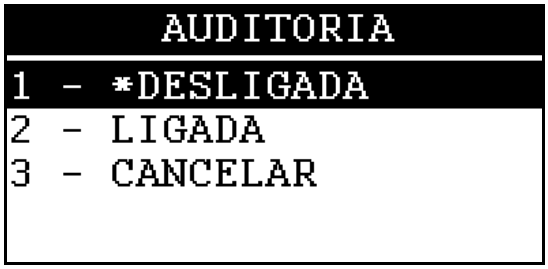


Figura 72 – Tela de configuração do tempo de acionamento da saída auxiliar

HABILITAR - configura o dispositivo para o armazenamento de eventos de auditoria.

DESABILITAR - configura o dispositivo para desconsiderar eventos de auditoria.

PROSSEGUIR – Segue para a próxima etapa do processo de configuração

CANCELAR – Finaliza a operação sem alterar as configurações

Finalmente para alterar as configurações o usuário deve confirmar.

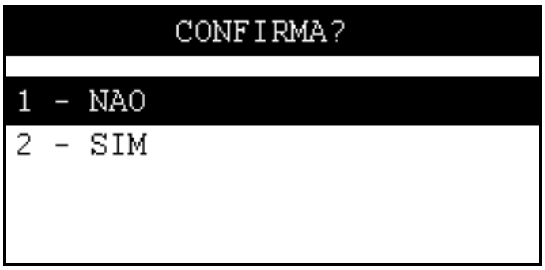


Figura 73 – Tela de confirmação da configuração da auxiliar

Após a confirmação será mostrada uma tela com o resultado da operação.

9.11.4.2 Maximo de eventos

Esta função pode ligar ou desligar o armazenamento de eventos de auditoria do sistema.

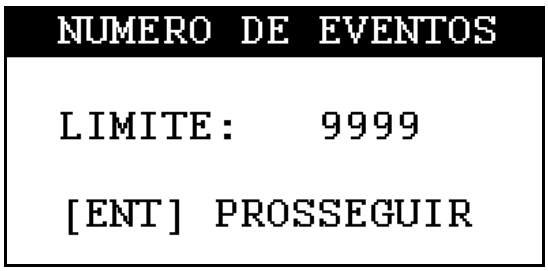


Figura 74 – Tela de configuração do Máximo de eventos

HABILITAR - configura o dispositivo para o armazenamento de eventos de auditoria.

DESABILITAR - configura o dispositivo para desconsiderar eventos de auditoria.

PROSSEGUIR – Segue para a próxima etapa do processo de configuração

CANCELAR – Finaliza a operação sem alterar as configurações

Finalmente para alterar as configurações o usuário deve confirmar.

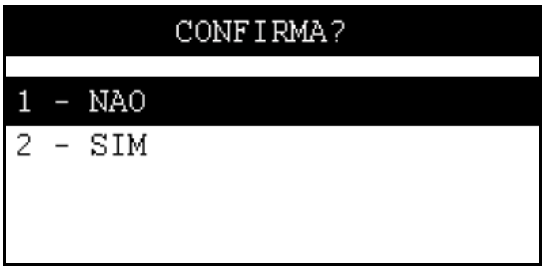


Figura 75 – Tela de confirmação da configuração da auxiliar

Após a confirmação será mostrada uma tela com o resultado da operação.

9.11.4.3 Limpeza de eventos

Esta função limpa a memória dos eventos já gravados no dispositivo. Para limpar os eventos basta que o usuário confirme a operação.

Antes de apagar os dados, recomenda-se fazer a coleta dos mesmos. Para maiores informações, consultar a seção 9.13 - Menu Listas.

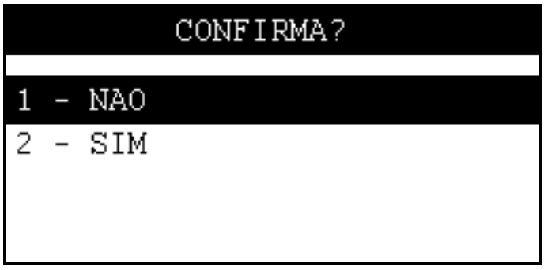


Figura 76 – Tela de confirmação da limpeza de eventos de auditoria

Após a confirmação será mostrada uma tela com o resultado da operação.

9.11.5 Status da porta

Esta função mostra ao usuário qual o estado das entradas do dispositivo, facilitando a instalação e manutenção.

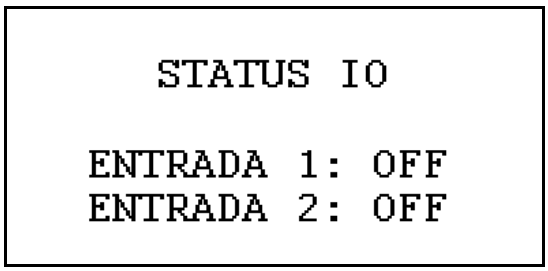


Figura 77 – Tela de status da porta

9.11.6 Menu Tela Principal

Contém as funções para mudança das mensagens localizadas na tela inicial do dispositivo.

Abaixo vemos como estão dispostas as mensagens configuradas pelo usuário:

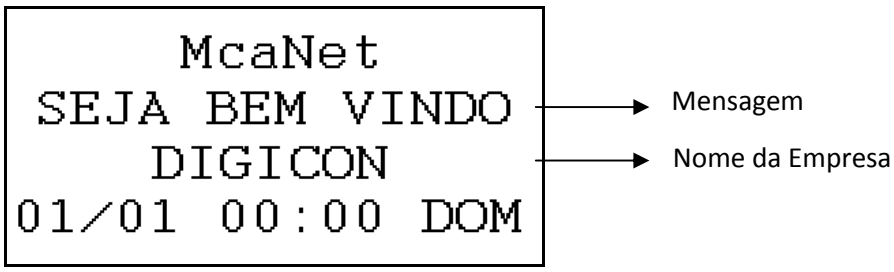


Figura 78 – Tela Inicial

9.11.6.1 Nome Empresa

Esta função altera o campo de nome da empresa na tela inicial do dispositivo.

O campo para preenchimento do nome da empresa é um campo alfanumérico, e sua digitação segue o mesmo modelo de digitação de um telefone comum. O teclado possui em cada uma das teclas, a impressão da relação de caracteres disponíveis na mesma.

Por exemplo a tecla dois (2), se pressionada uma vez, exibe o caractere 'A', se pressionada duas vezes o caractere 'B', se pressionada três vezes o caractere 'C' e se pressionada quatro vezes o número 2.

Para apagar o último caractere digitado, basta pressionar a tecla CLR, e para finalizar a digitação no campo, basta digitar a tecla ENT.

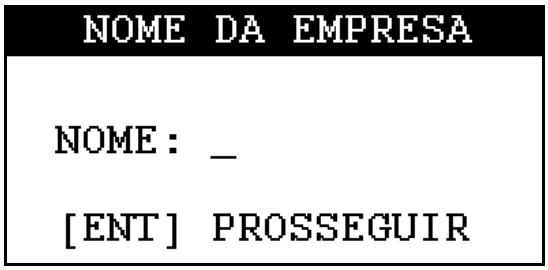


Figura 79 – Tela de alteração do nome da empresa

Após a escolha do nome da empresa, o usuário deve pressionar a tecla ENT ou ESC para cancelar a operação.

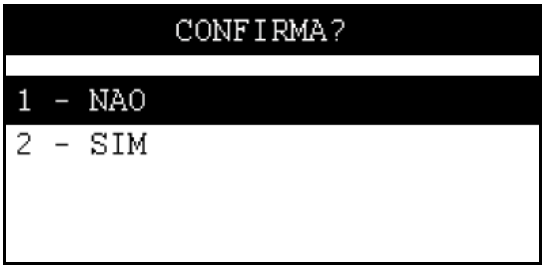


Figura 80 – Tela de confirmação de alteração do nome de empresa

Para aplicar as configurações o usuário deverá confirmar.

9.11.6.2 Mensagem Tela

Serve para alteração da mensagem de boas-vindas na tela ou simplesmente identificar a localidade guardada.

O campo para preenchimento da mensagem em tela é um campo alfanumérico, e sua digitação segue o mesmo modelo de digitação de um telefone comum. O teclado possui em cada uma das teclas, a impressão da relação de caracteres disponíveis na mesma.

Por exemplo a tecla dois (2), se pressionada uma vez, exibe o caractere 'A', se pressionada duas vezes o caractere 'B', se pressionada três vezes o caractere 'C' e se pressionada quatro vezes o número 2.

Para apagar o último caractere digitado, basta pressionar a tecla CLR, e para finalizar a digitação no campo, basta digitar a tecla ENT.

Ao acessar o usuário será apresentado à tela de entrada da mensagem:

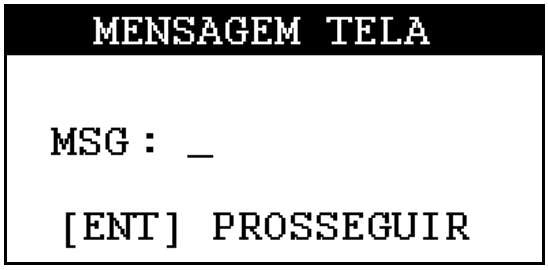


Figura 81 – Tela de alteração de mensagem

Ao finalizar a entrada dos dados, o usuário deve confirmar a alteração:

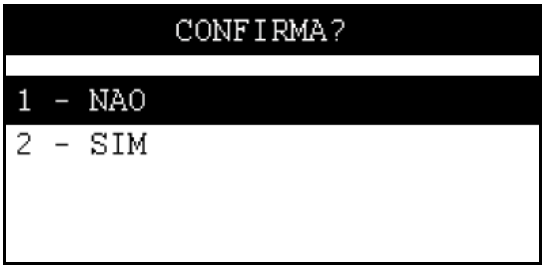


Figura 82 – Tela de confirmação de alteração de mensagem de tela

Após a confirmação será mostrada uma tela com o resultado da operação.

9.11.7 ID do equipamento

A identificação do equipamento é utilizada para reconhecimento do dispositivo quando utilziada uma aplicação para configuração do mesmo em rede. O dispositivo é

identificado por IP, mas a alteração destes nomes permite que o usuário da aplicação esteja ciente da localidade que está configurando.

A APLICAÇÃO DE CONTROLE É DESCRITA EM DOCUMENTAÇÃO SEPARADA.

Os campos para preenchimento do ID e do local são um campos alfanuméricos, e sua digitação segue o mesmo modelo de digitação de um telefone comum. O teclado possui em cada uma das teclas, a impressão da relação de caracteres disponíveis na mesma.

Por exemplo a tecla dois (2), se pressionada uma vez, exibe o caractere 'A', se pressionada duas vezes o caractere 'B', se pressionada três vezes o caractere 'C' e se pressionada quatro vezes o número 2.

Para apagar o último caractere digitado, basta pressionar a tecla CLR, e para finalizar a digitação no campo, basta digitar a tecla ENT.

Ao acessar a função será apresentada uma tela para alteração dos dois parâmetros. Para prosseguir o usuário deve preencher ambos os campos e pressionar a tecla ENT, ou pressionar a tecla ESC para cancelar a operação.

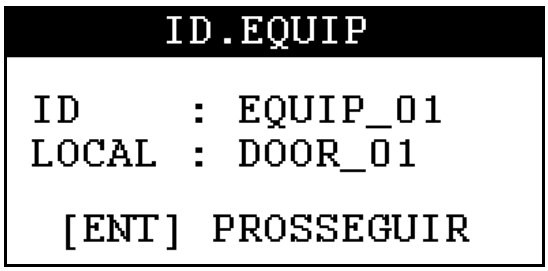


Figura 83 – Tela de alteração de Id do equipamento

Dois parâmetros são necessários:

ID – Identificador do equipamento

LOCAL – Identificador da localidade do equipamento

Estes parâmetros servem para agrupar os dispositivos, facilitando sua identificação.

Ao finalizar a entrada dos dados, o usuário deve confirmar a alteração:

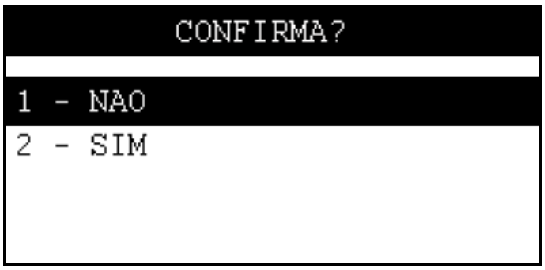


Figura 84 – Tela de confirmação de alteração de Id do equipamento

Após a confirmação será mostrada uma tela com o resultado da operação.

9.11.8 Beep Teclado

Esta função liga ou desliga os sons do teclado. Quando ligado, ao pressionar uma tecla será gerado um tom.

Para alterar a configuração, o usuário deve escolher a opção desejada, ou cancelar caso não deseje alterar a configuração:

Figura 85 – Tela de confirmação de alteração de Id do equipamento

Após a escolha de uma das opções o usuário deverá confirmar para alterar a configuração:

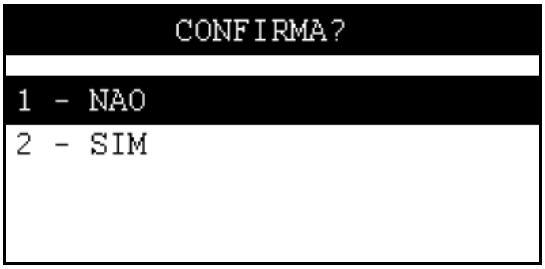


Figura 86 – Tela de confirmação de alteração de Id do equipamento

Após a tela de confirmação será mostrada uma tela com o resultado da operação.

9.11.9 Soft Reset

Esta função reinicia a aplicação.

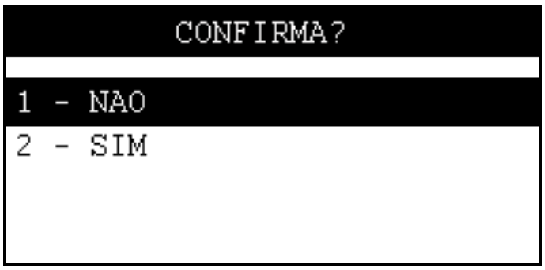


Figura 87 – Tela de confirmação de reset da aplicação

Após a confirmação será mostrada uma tela com o resultado da operação, e a aplicação será reiniciada.

Esta operação não altera nenhuma configuração do equipamento nem altera dados no dispositivo, servindo apenas para finalizar e reiniciar o apicativo.

Sua funcionalidade principal é basicamente de auxílio à manutenção, e é de maior importância em situações como a atualização de firmware, que requer que a aplicação não esteja sendo utilizada (para maiores informações, consultar a seção 9.8 - Atualização de firmware do dispositivo).

9.11.10 Menu Backup

Contém funções relativas ao backup e restauração de dados do dispositivo.

9.11.10.1 Criar Backup

Esta função realiza um backup (cópia) dos dados presentes no dispositivo. Todos os dados relativos á cadastro e configuração no momento em que for realizado serão gravados em um dispositivo de armazenamento USB.

Os arquivos com os dados do backup serão colocados em uma pasta cujo nome é uma marca de tempo, para que o usuário saiba quando foi feito o backup. A marca de tempo de formato:

AAAAMMDDhhmm

, aonde:

AAAA – ANO

MM – Mês

DD – Dia

Hh – Hora

Mm – Minuto

Por exemplo, um backup criado no dia 23/04/2010, ás 14h35min teria o seguinte formato:

201004231435

Do mesmo modo, os arquivos de backup são criados com a mesma marca de tempo para evitar que sejam confundidos com backups de outras datas.

Cada arquivo gerado possui um bloco de dados, e para a restauração correta é necessário que os três arquivos sejam utilizados em conjunto.

Os arquivos de biometria ficam guardados no arquivo com nome "mcabiobkp- AAAAMMDDhhmm.tar.gz", os arquivos de configuração são salvos no arquivo com nome "mcanet_ini- AAAAMMDDhhmm.tar.gz", e finalmente o backup da base de dados ficam guardados no arquivo de nome "mcadbbkp- AAAAMMDDhhmm.sql.tar.gz".

Para realizar o backup, primeiramente o usuário deve inserir a mídia na entrada USB presente na lateral do equipamento (vide seção 9.2 – Entrada USB). Após a inserção basta confirmar o backup e esperar a finalização da operação.

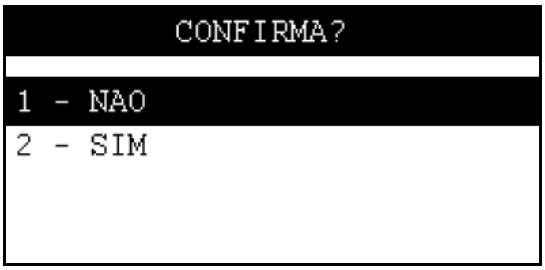


Figura 88 – Tela de confirmação de criação de backup

Após a confirmação será mostrada uma tela com o resultado da operação, para sair desta tela o usuário deve retirar o dispositivo.

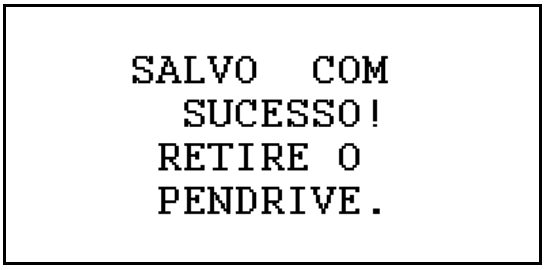


Figura 89 – Tela de sucesso na realização do backup

9.11.10.2 Restaurar Backup

A restauração do backup serve para recuperar dados gravados em um dispositivo de armazenamento USB previamente, apagando todos os dados existentes no dispositivo e substituindo-os pelos dados desejados.

Para escolher um ponto para restaurar o dispositivo, o usuário deve escolher um ponto de backup entre os que já tiverem sido feitos ao longo do tempo de vida do dispositivo (para maiores informações, consultar a seção 9.11.10.1 - Criar Backup).

ESCOLHIDO O PONTO DE RESTAURAÇÃO, O USUÁRIO DEVE COLOCAR TODOS OS TRÊS ARQUIVOS SEM A MARCE DE TEMPO DENTRO DE UMA PASTA DE NOME RESTORE, NA RAIZ DO DISPOSITIVO DE ARMAZENAMENTO. CASO NÃO SEJAM COLOCADOS TODOS OS TRÊS ARQUIVOS O BACKUP NÃO SERÁ REALIZADO E SERÀ APRESENTADA UMA MENSAGEM DE ERRO.

Por exemplo, se o usuário escolher o backup gerado em 23/04/2010, ás 14h35min, deve ir á pasta "backup/201004231435" na raiz do dispositivo e recolher os três arquivos ali presentes, de nome "mcabiobkp-201004231435.tar.gz", "mcanet_ini- 201004231435.tar.gz", "mcadbbkp- 201004231435.sql.tar.gz". Após este procedimento o usuário deve renomear os arquivos, somente retirando a marca de tempo de cada um. Assim os arquivos serão renomeados do seguinte modo:

mcabiobkp-201004231435.tar.gz → mcabiobkp.tar.gz

mcanet_ini- 201004231435.tar.gz → mcanet_ini.tar.gz

mcadbbkp- 201004231435.sql.tar.gz → mcadbbkp.sql.tar.gz

Após ter os arquivos renomeados colocados no diretório correto, o usuário pode prosseguir com a operação.

Para realizar a restauração, primeiramente o usuário deve inserir a mídia na entrada USB presente na lateral do equipamento (vide seção 9.2 – Entrada USB), sendo que esta mídia deve conter um backup feito previamente (pelo mesmo dispositivo ou por um dispositivo MCANet que contenha os mesmos dispositivos de autorização), como mencionado nos parágrafos anteriores. Após a inserção basta confirmar a restauração e esperar a finalização da operação.

Esta operação requer mais tempo do que o backup, e **A NÃO SER QUE O DISPOSITIVO DEMORE MAIS DO QUE 20 MINUTOS PARA REALIZAR A RESTAURAÇÃO, NÃO É RECOMENDADO RETIRAR A MÍDIA OU DESLIGAR O DISPOSITIVO SOB PENA DE CORROMPER OS DADOS DA APLICAÇÃO. O TEMPO UTILIZADO PELO DISPOSITIVO PARA A RESTAURAÇÂO DEPENDE DA QUANTIDADE DE DADOS GRAVADOS NO DISPOSITIVO NO MOMENTO EM QUE FOI REALIZADO O BACKUP.**

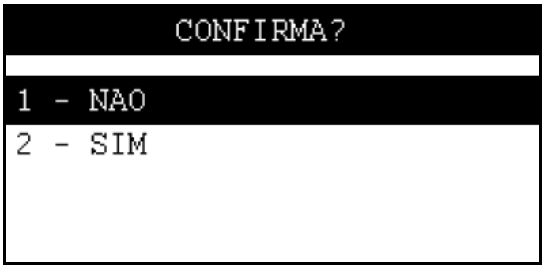


Figura 90 – Tela de confirmação de restauração de backup

Após a confirmação será mostrada uma tela com o resultado da operação, para sair desta tela o usuário deve retirar o dispositivo.

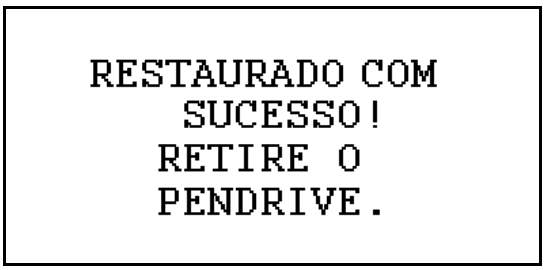


Figura 91 – Tela de sucesso na realização da restauração

O dispositivo será reiniciado após a restauração, com os dados já restaurados.

9.12 Menu Cadastro

Neste Menu estão as opções relativas ao cadastro de usuários e datas.

9.12.1 Menu Usuário

Contém operações relativas ao cadastro individual de usuários para cada dispositivo.

9.12.1.1 Seleção de usuários

Para a alteração de informações de usuário (inclusão, exclusão e consulta), será sempre mostrada uma etapa de seleção de usuário. Pode-se fazer isto de duas maneiras, através da digitação do ID do usuário ou da escolha em uma lista dos usuários cadastrados.

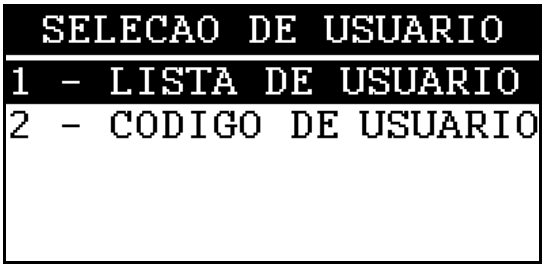


Figura 92 – Tela de opção de escolha de usuário

Na opção LISTA DE USUARIO, serão apresentados todos os usuários cadastrados em uma lista para que se escolha qual deles será cadastrado com o identificador selecionado.

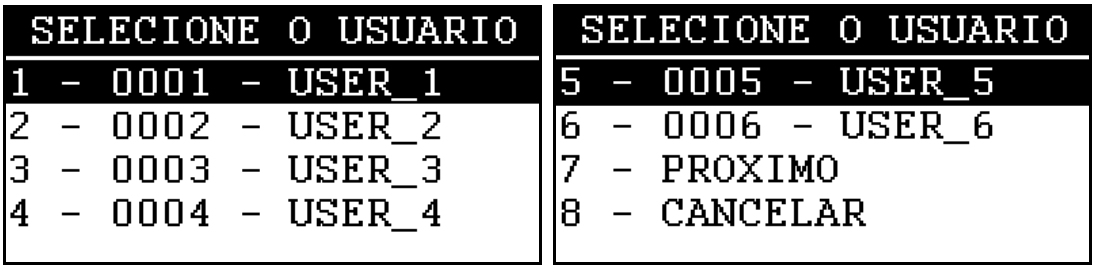

SELECIONE O USUARIO
1 - 0001 - USER_1
2 - 0002 - USER_2
3 - 0003 - USER_3
4 - 0004 - USER_4
SELECIONE O USUARIO
5 - 0005 - USER_5
6 - 0006 - USER_6
7 - PROXIMO
8 - CANCELAR

Figura 93 – Lista de escolha de usuário

A lista de usuários, se muito grande será mostrada em várias telas, e para navegar nelas, basta selecionar a opção PROXIMO ou VOLTAR. Os usuários são mostrados seguindo a ordem de seus IDs.

Na opção CODIGO DE USUARIO, pode-se digitar o ID desejado para cadastro diretamente.

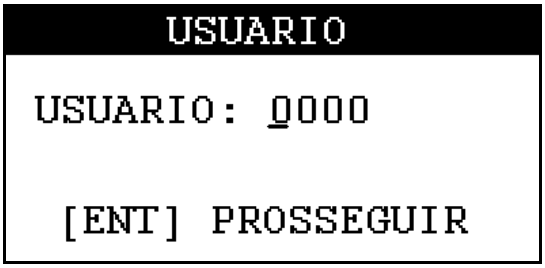


Figura 94 – Escolha de usuário por ID

Em todos os casos, se o usuário já possuir cadastro no modo de acesso selecionado, será mostrada uma tela de erro.

9.12.1.2 Menu Incluir

Seção de funções relativas á inclusão de novos usuários e identificadores. Nem todos os dispositivos listados nesta função podem estar presentes no dispositivo MCANet. Neste caso será mostrada uma mensagem indicando que o dispositivo não está instalado:

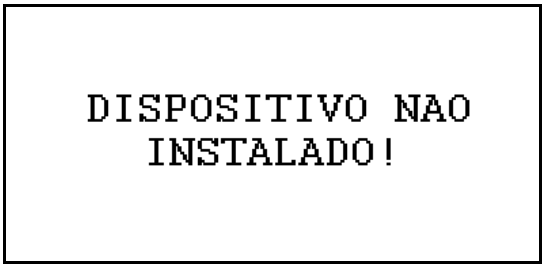


Figura 95 – Dispositivo não instalado

Um usuário que esteja cadastrado no dispositivo de autenticação escolhido para inclusão receberá uma mensagem de erro indicando que já possui este tipo de informações de acesso. Um exemplo seria a tentativa de cadastro de biometria para um usuário que jápossui biometria:

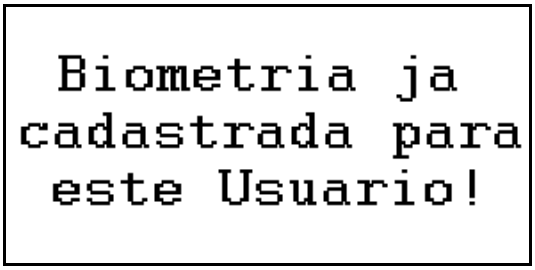


Figura 96 –Biometria já cadastrada

9.12.1.2.1 ID/Senha

Nesta função pode-se criar um novo usuário, fornecendo a ele um novo ID, nome e perfil de acesso.

Primeiramente deve-se definir um perfil de acesso:

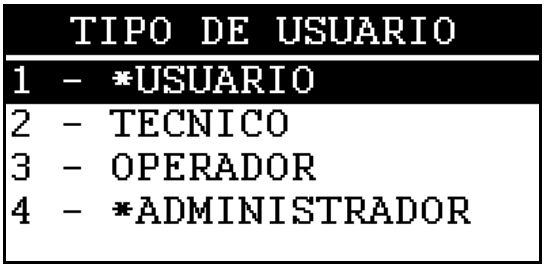


Figura 97 – Tela de escolha do perfil

O usuário deve se lembrar que somente um administrador pode criar outro administrador, sendo vetado ao operador a criação de usuários com perfil de administrador.

As opções presentes são:

1 – Usuário – Permite acesso ao local, e pode ser combinado com qualquer dos outros três abaixo (os perfis de técnico, usuário e operador não podem ser combinados entre si),. Permite também acesso ao menu do usuário (vide seção 9.4 – Menu do Usuário para verificar as permissões deste perfil).

2 – Técnico – Permite acesso ao menu de técnico (vide seção 9.5 – Menu do Técnico para verificar as permissões deste perfil).

3 – Operador - Permite acesso ao menu de técnico (vide seção 9.6 – Menu do Operador para verificar a s permissões deste perfil).

4 – Administrador - Permite acesso ao menu de técnico (vide seção 9.7 – Menu do Administrador para verificar a s permissões deste perfil).

5 – Cancelar – Volta ao menu

6 – Finalizar – Finaliza a escolhas do perfil e passa à próxima etapa

Ao selecionar um perfil este será marcado em tela e ao selecionar a opção 6 os perfis marcados corresponderão ao perfil do cadastro.

A próxima tela serve para o cadastro de ID de usuário e senha:

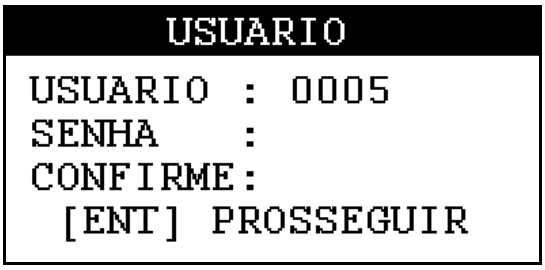


Figura 98 – Tela de escolha do ID de usuário

Será sempre mostrado em tela, como sugestão de ID o número de identificação mais baixo ainda não cadastrado, no entanto o usuário pode alterar esta informação digitando a tecla CLR.

A seguir o usuário deve escolher o nome para a identificação criada. Novamente será criado um nome de sugestão para o usuário criado, baseado em seu ID. Para alterar esta escolha, utilizar a tecla CLR para limpar o campo.

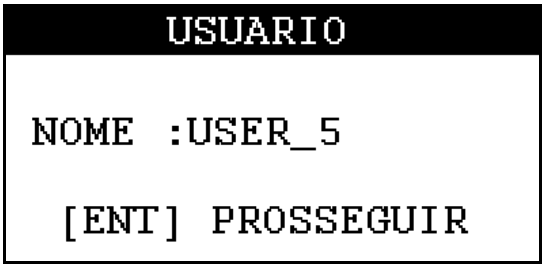


Figura 99 – Tela de escolha do nome de usuário

Finalmente após confirmar esta informação, será mostrada uma tela com o resultado da operação.

9.12.1.2.2 Biometria

O cadastro de biometrias requer a presença do usuário para o qual a mesma será cadastrada.

Primeiramente, deve-se escolher o usuário para o qual será cadastrada a biometria (vide seção 9.12.1.1 – Seleção de Usuários).

Após a escolha do usuário, poderá começar o processo de cadastro. Caso o usuário já esteja cadastrado, será mostrada uma tela de erro.

Caso o usuário não tenha biometria cadastrada, será iniciado o procedimento de captura da biometria.

Dependendo do modelo de sensor presente no MCANet, será requisitado ao usuário que o mesmo coloque sua digital no sensor biométrico duas ou três vezes (para saber aonde está localizado o sensor e como utiliza-lo, verifique a seção 9.1.1 – Sensor Biométrico de digitais).

Dois ciclos de identificação serão iniciados, e para cada um deles deve ser utilizada uma digital diferente do mesmo usuário, ou seja, por usuário teremos duas digitais cadastradas.

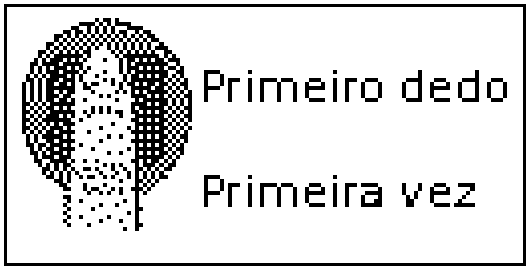


Figura 100 – Cadastro da primeira digital

O usuário deve ficar atento a mudança entre as duas digitais. Será mostrado em tela quando o usuário deve passar para o próximo dedo.

Figura 101 – Cadastro da segunda digital

Entre cada captura de digital, será mostrada uma tela indicando ao usuário que este pode retirar o dedo do sensor.

Figura 102 – Requisição de retirada do dedo do sensor

Caso as instruções acima não sejam seguidas, o usuário corre o risco de ter a digital cadastrada erroneamente, caso isto aconteça, a biometria cadastrada deve ser excluída e cadastrada novamente (vide seção 9.12.1.3.2 –exclusão de biometria).

9.12.1.2.3 Código de Barras

Primeiramente, deve-se escolher o usuário para o qual será cadastrada o cartão com código de barras (vide seção 9.12.1.1 – Seleção de Usuários).

Caso o usuário não tenha cartão de código de barras cadastrado, será iniciado o procedimento de captura do código do cartão.

Quando requisitado, o usuário deve passar o cartão na fenda de leitura de código de barras (vide seção 9.1.2 – Leitor de Código de Barras).

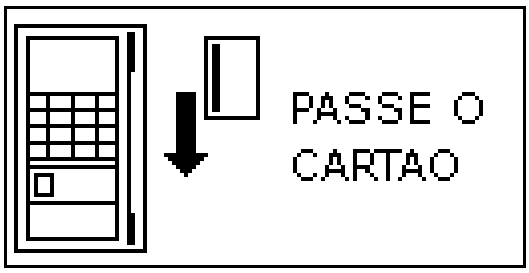


Figura 103 – Tela de cadastro de Código de barras

Após o fim da operação será mostrada uma tela com o resultado da operação.

9.12.1.2.4 RFID

Primeiramente, deve-se escolher o usuário para o qual será cadastrada o cartão RFID (vide seção 9.12.1.1 – Seleção de Usuários).

Caso o usuário não tenha cartão RFID cadastrado, será iniciado o procedimento de captura do código do cartão.

Quando requisitado, o usuário deve aproximar o cartão da área de leitura (vide seção 9.1.3 – Leitor de cartões MIFARE e RFID).

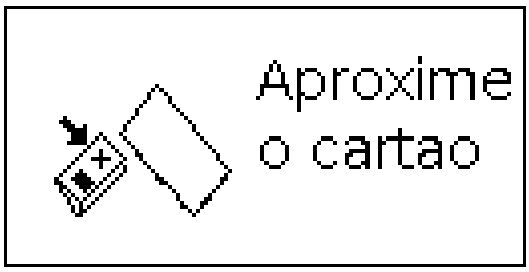


Figura 104 – Tela de cadastro de RFID

Após o fim da operação será mostrada uma tela com o resultado da operação.

9.12.1.2.5 MIFARE

Primeiramente, deve-se escolher o usuário para o qual será cadastrada o cartão MIFARE (vide seção 9.12.1.1 – Seleção de Usuários).

Caso o usuário não tenha cartão MIFARE cadastrado, será iniciado o procedimento de captura do código do cartão.

Quando requisitado, o usuário deve aproximar o cartão da área de leitura (vide seção 9.1.3 – Leitor de cartões MIFARE e RFID).

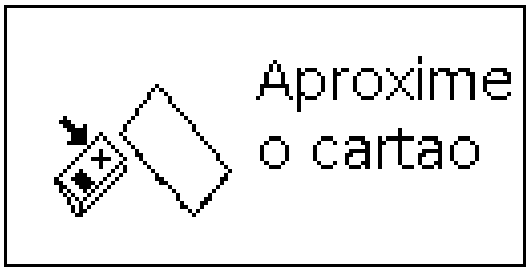


Figura 105 – Tela de cadastro de MIFARE

Após o fim da operação será mostrada uma tela com o resultado da operação.

9.12.1.2.6 MIFARE+Biometria

Primeiramente, deve-se escolher o usuário para o qual será cadastrada o cartão MIFARE com biometria (vide seção 9.12.1.1 – Seleção de Usuários).

Caso o usuário não tenha cartão MIFARE cadastrado, será iniciado o procedimento de captura do código do cartão.

Primeiramente será capturado o modelo de biometria do usuário. O procedimento é bastante parecido com o cadastro de biometria, mas no caso do MIFARE com biometria será cadastrado somente um dedo de cada usuário.

Quando for requisitado, o usuário deve inserir o dedo no sensor de biometria(para saber aonde está localizado o sensor e como utiliza-lo, verifique a seção 9.1.1 – Sensor Biométrico de digitais).

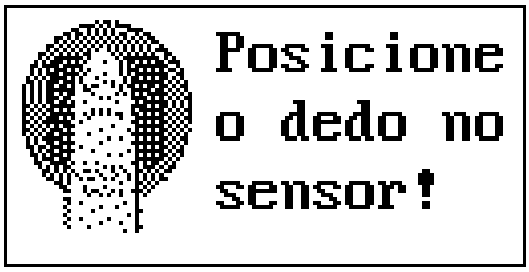


Figura 106 – Tela de captura de modelo de biometria

Quando requisitado, o usuário deve aproximar o cartão da área de leitura (vide seção 9.1.3 – Leitor de cartões MIFARE e RFID).

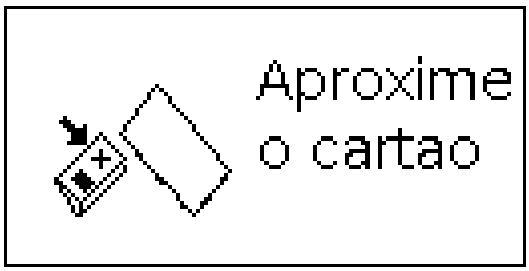


Figura 107 – Tela de gravação de biometria no MIFARE

O usuário deve manter o cartão próximo à área de leitura até que seja mostrada a tela com o resultado da operação.

9.12.1.2.7 Horário de Visita

O horário de visita é cadastrado para que o usuário tenha acesso em dias fora de seu cadastro padrão. É válido somente no dia cadastrado.

Primeiramente o usuário deverá cadastrar um dia para a entrada:

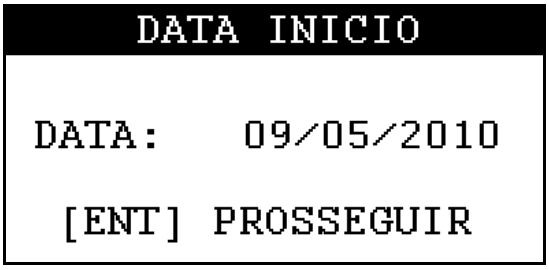


Figura 108 – Tela de escolha da data para visita

Após a entrada da data, o usuário deve pressionar ENT para prosseguir com a entrada da hora ou ESC para voltar ao menu.

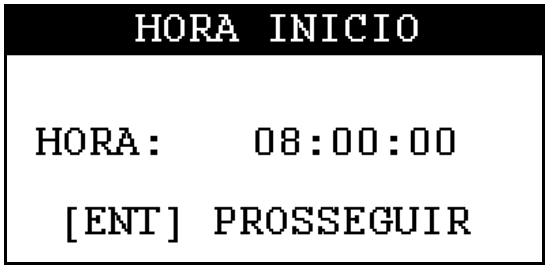


Figura 109 – Tela de escolha da hora inicial da visita

O próximo passo é a escolha da data para o fim da visita:

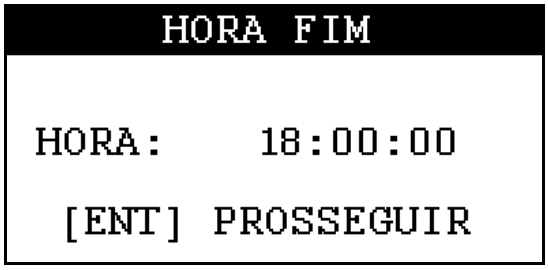


Figura 110 – Tela de escolha da hora inicial da visita

Após o fim da operação será mostrada uma tela com o resultado.

9.12.1.3 Menu Deletar

Este menu contem funções de exclusão de informações de acesso e datas individuais de usuários.

Como as regras do sistema dão acesso pleno somente ao usuário administrador e sendo somente este perfil capaz de cadastrar outros usuários, o sistema não permitirá que um administrador seja excluído, se este for o único administrador ativo no sistema.

Também seguindo o mesmo princípio, não é possível deletar qualquer uma das informações de acesso de um dispositivo ativo para autorização se somente um administrador tiver uma informação deste tipo cadastrada.

9.12.1.3.1 ID/Senha

Este função exclui um usuário previamente cadastrado no sistema. Todos os seus dados serão apagados no momento em que sua exclusão for confirmada.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha, tudo que o usuário tem a fazer é confirmar a exclusão dos dados.

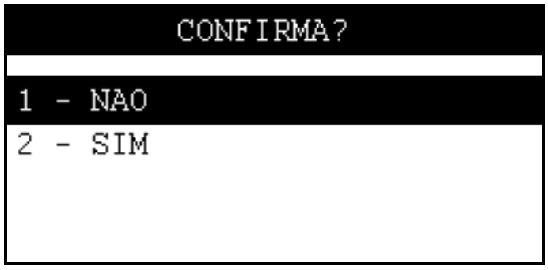


Figura 111 – Confirmação de exclusão de usuário

Após a seleção será mostrada uma tela com o resultado da operação.

9.12.1.3.2 Biometria

Este função exclui a informação de biometria previamente cadastrada para um usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha será mostrada uma tela com o resultado da operação.

9.12.1.3.3 Código de Barras

Este função exclui a informação de código de barras previamente cadastrada para um usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha será mostrada uma tela com o resultado da operação.

9.12.1.3.4 RFID

Este função exclui a informação de cartão RFID previamente cadastrada para um usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha será mostrada uma tela com o resultado da operação.

9.12.1.3.5 MIFARE

Este função exclui a informação de cartão MIFARE previamente cadastrada para um usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha será mostrada uma tela com o resultado da operação.

9.12.1.3.6 Horário de Visita

Este função exclui uma data de visita previamente cadastrada para um usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento de escolha será mostrada uma lista com as visitas cadastradas para cada usuário:

Figura 112 – Tela de escolha de datas de visita

Após selecionar a data para exclusão, o usuário deve confirmar a escolha.

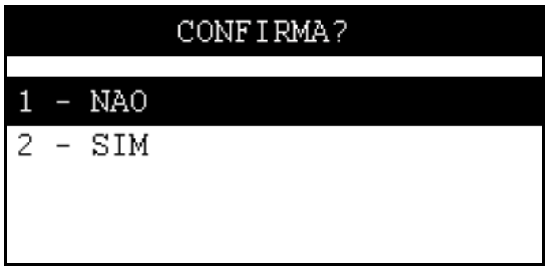


Figura 113 – Confirmação de exclusão de visita

Ao final da operação será mostrada uma tela com o resultado.

9.12.1.4 Menu Alterar

Este menu serve para alterar configurações de usuários já existentes.

9.12.1.4.1 Menu Password

Para alterar o password do usuário logado ao menu no momento escolha a função USUARIO ATUAL, senão escolha OUTRO USUARIO.

9.12.1.4.1.1 Usuario atual

Para alterar a senha do usuário, basta digitar a senha atual do usuário, a nova senha e a confirmação da nova senha.

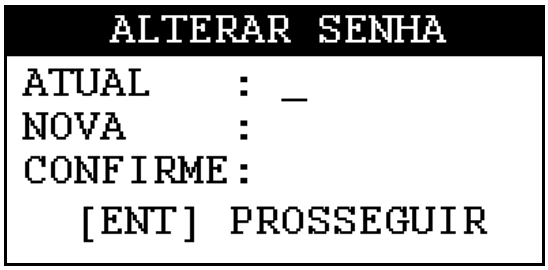


Figura 114 – Alteração da própria senha de usuário

Para finalizar basta confirmar a operação.

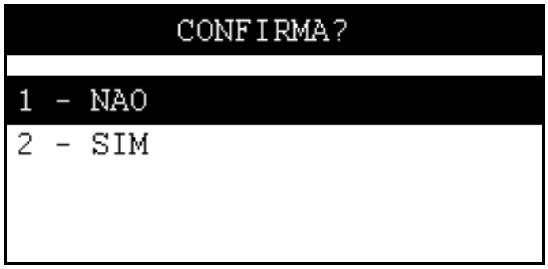


Figura 115 – Confirmação de alteração da própria senha de usuário

9.12.1.4.1.2 *Outro Usuario*

Esta função altera a senha de um usuário que não seja o logado no momento.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após o procedimento será mostrada uma tela com dois campos, nos quais serão digitados a nova senha do usuário escolhido.

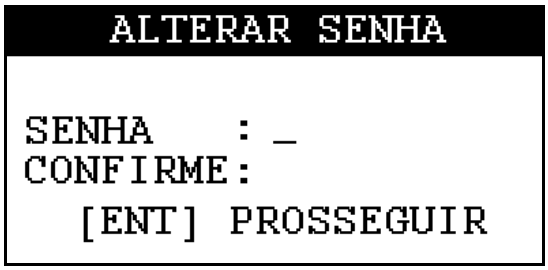


Figura 116 – Alteração de senha de usuário

Para finalizar basta confirmar a operação.

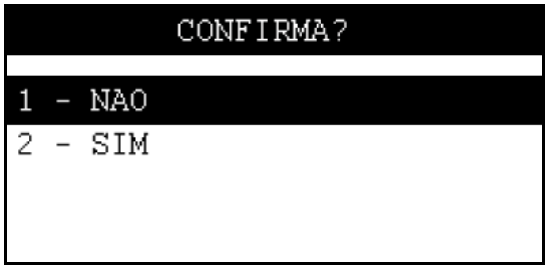


Figura 117 – Confirmação de alteração de senha de usuário

Após o fim da operação será mostrada uma tela com o resultado.

9.12.1.4.2 *Status*

Esta função altera o status de um usuário. Usuários que não estejam com status ATIVO não terão permissão para acesso a nenhuma funcionalidade do sistema, e os outros status servem apenas para diferenciar um motivo de afastamento do usuário.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após este procedimento será mostrada uma tela com as possibilidades de escolha para novo estado do usuário.

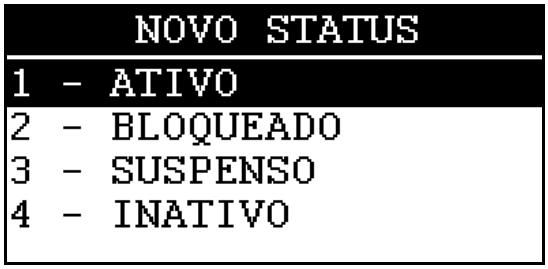


Figura 118 – Alteração de senha de usuário

Os status Para seleção são:

ATIVO, BLOQUEADO, SUSPENSO, INATIVO e AUSENTE.

Após selecionar um estado, será pedida automaticamente uma confirmação para operação.

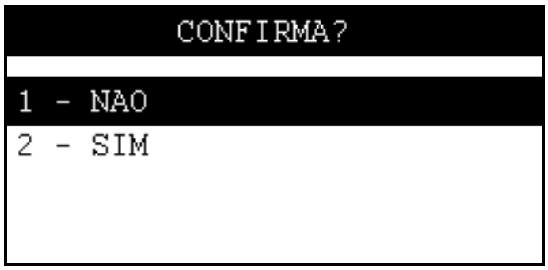


Figura 119 – Confirmação de alteração de senha de usuário

Após o fim da operação será mostrada uma tela com o resultado.

9.12.1.4.3 Perfil

A alteração de perfil atualiza as permissões de acesso do usuário alvo da operação, e pode ser feita somente por um administrador.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após este procedimento será mostrada uma tela com as possibilidades de escolha para novo perfil do usuário.

Após a escolha do usuário deve-se escolher um novo perfil de acesso:

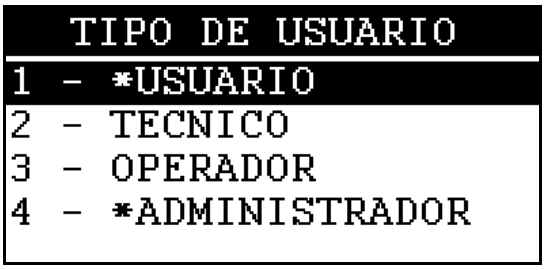


Figura 120 – Tela de escolha do perfil

As opções presentes são:

1 – Usuário – Permite acesso ao local, e pode ser combinado com qualquer dos outros três abaixo (os perfis de técnico, usuário e operador não podem ser combinados entre si),. Permite também acesso ao menu do usuário (vide seção 9.4 – Menu do Usuário para verificar as permissões deste perfil).

2 – Técnico – Permite acesso ao menu de técnico (vide seção 9.5 – Menu do Técnico para verificar as permissões deste perfil).

3 – Operador - Permite acesso ao menu de técnico (vide seção 9.6 – Menu do Operador para verificar a s permissões deste perfil).

4 – Administrador - Permite acesso ao menu de técnico (vide seção 9.7 – Menu do Administrador para verificar a s permissões deste perfil).

5 – Cancelar – Volta ao menu

6 – Finalizar – Finaliza a escolhas do perfil e passa à próxima etapa

Ao selecionar um perfil este será marcado em tela e ao selecionar a opção 6 os perfis marcados corresponderão ao perfil do cadastro.

Após selecionar um novo perfil e selecionada a opção FINALIZAR, será pedida a confirmação da operação.

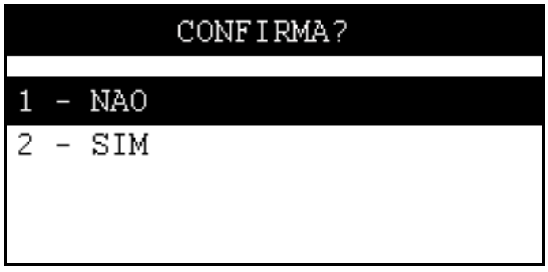


Figura 121 – Confirmação de alteração de senha de usuário

Após o fim da operação será mostrada uma tela com o resultado.

9.12.1.4.4 Nome

Esta função somente altera o identificador secundário que é o nome de usuário. A alteração de nome não modifica o acesso do mesmo, e dois usuários podem ter o mesmo nome.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após este procedimento será mostrada uma tela com o formulário de entrada do nome:

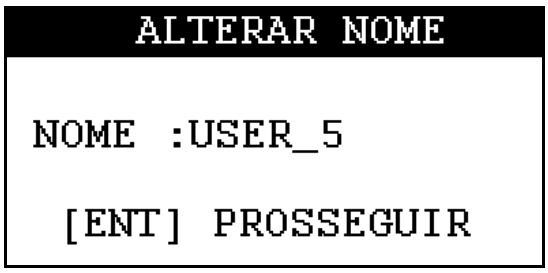


Figura 122 – Alteração de nome de usuário

Após selecionar um novo nome e pressionada a tecla ENT, será pedida a confirmação da operação. O usuário pode cancelar a operação pressionando a tecla ESC.

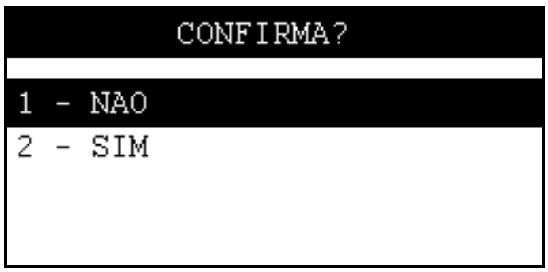


Figura 123 – Confirmação de alteração de nome de usuário

Após o fim da operação será mostrada uma tela com o resultado.

9.12.1.4.5 *Período de Acesso*

Esta opção configura o período de acesso de um usuário, existe também uma opção no menu de configuração para alteração do período de acesso. O usuário deve ter cuidado para não confundir as duas funções, sendo que a função presente no menu configuração cuida somente dos horários para os quais um novo usuário será cadastrado, e a função presente no menu alterar

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após este procedimento será mostrada uma tela questionado ao usuário quais dias da semana serão liberados:

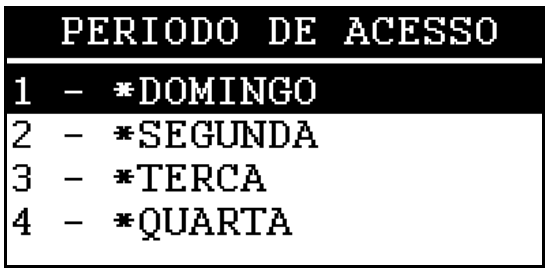


Figura 124 – Configuração de período – dias da semana

Para selecionar um dia, basta apertar ENT ou a numeração ao lado do dia selecionado. Dias selecionados serão marcados por um '*' ao lado, e podem ser desmarcados, bastando seleciona-los novamente.

O próximo passo é escolher o hoário de acesso, sendo a tela a seguir a tela para escolha da hora de início do período.

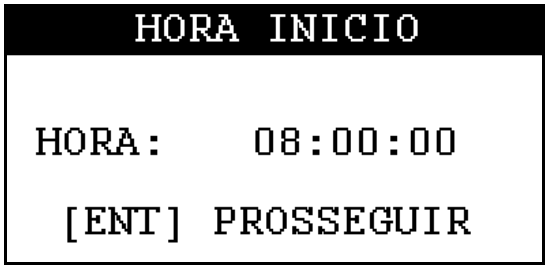


Figura 125 – Configuração de período – hora início

Nesta tela o usuário deve selecionara a hora de início, e após o término do preenchimento deve pressionar a tecla ENT.

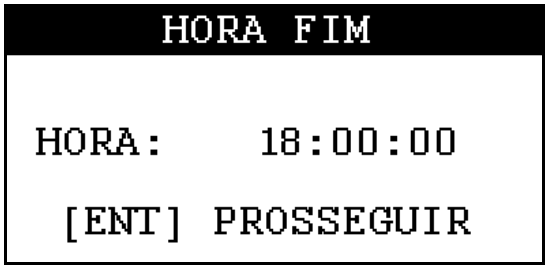


Figura 126 – Configuração de período – hora fim

Na próxima tela o usuário deve escolher a hora de fim do período, e após o término do preenchimento deve presionar a tecla ENT.

A próxima tela é para escolha da data de fim do período (após esta data, um usuário cadastrado segundo estas configurações não terá mais acesso, a não ser que o período de acesso do mesmo especificamente seja alterado).

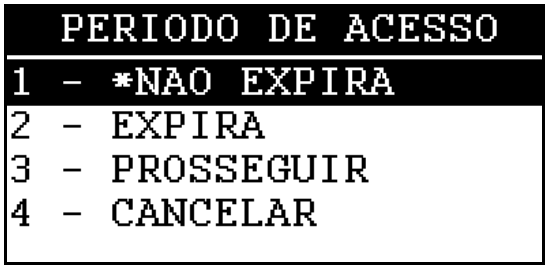


Figura 127 – Configuração de período – expiração

Nesta tela a opção desejada estará marcada.

A opção NÃO EXPIRA faz com que o usuário tenha permissão para acesso (dentro dos dias e horas cadastrados) sem data para expiração de acesso, e finaliza a operação.

A opção EXPIRA segue para uma tela aonde o usuário deve escolher um prazo para expiração do tempo de acesso em semanas.

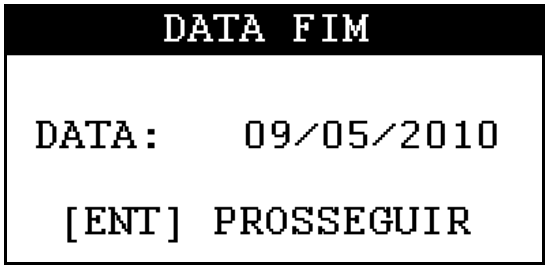


Figura 128 – Configuração de período – Data para expiração

Após a escolha do período para o fim a operação será finalizada.

A opção PROSSEGUIR executa a opção selecionada pelo usuário.

A opção CANCELAR sai da função sem salvar as alterações.

Após o fim da operação será exibida uma tela com o resultado final da operação.

9.12.2 Menu Datas

Este menu contem as funções para gerenciamento de datas de feriado e configuração do dispositivo.

9.12.2.1 Agendar Configuração

O agendamento de configuração serve para permitir que um técnico acesse o menu. O perfil de técnico pode executar mudanças de configuração no sistema somente quando estiver agendado um horário de configuração e o acesso estiver sendo feito no período informado.

A escolha do usuário é o primeiro passo (vide seção 9.12.1.1 – Seleção de Usuários), e após este procedimento será mostrada uma tela para configuração da data e hora de início do período:

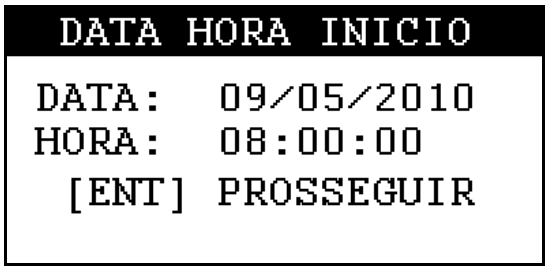


Figura 129 – Agendamento de manutenção – Data e hora de início

Será sempre dada como sugestão a data e hora atuais. Pra apagar os dados, caso a sugestão não correponda á vontade do usuário, pressionar a tecla CLR.

Após a configuração da data de início, será questionada a data e hora de fim do período:

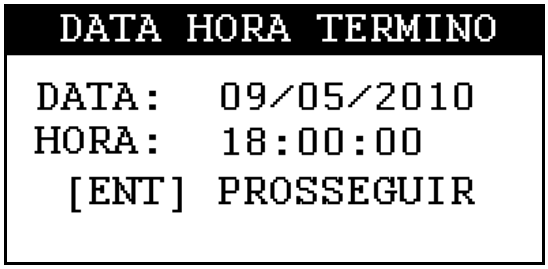


Figura 130 – Agendamento de manutenção – Data e hora de início

Para finalizar a operação, o usuário deve confirmar. Logo após será mostrada uma tela com o resultado da operação.

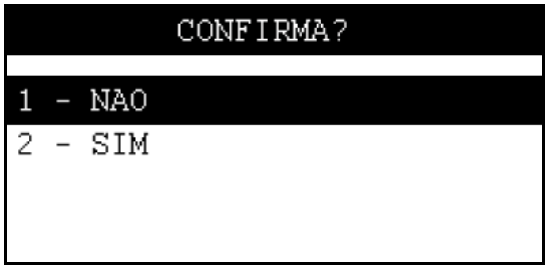


Figura 131 – Confirmação de Agendamento de manutenção

9.12.2.2 Feriado

Esta função cadastra um dia para o qual os acessos não serão permitidos para todos os uauários.

Primeiramente deve ser configurada a data e hora de início do período:

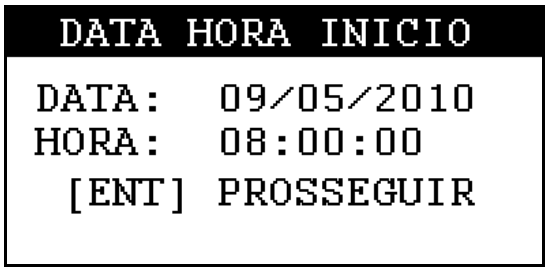


Figura 132 – Agendamento de manutenção – Data e hora de início

Será sempre dada como sugestão a data e hora atuais. Pra apagar os dados, caso a sugestão não correponda á vontade do usuário, pressionar a tecla CLR.

Após a configuração da data de início, será questionada a data e hora de fim do período:

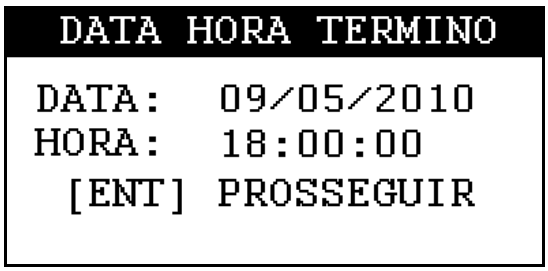


Figura 133 – Agendamento de manutenção – Data e hora de início

Para finalizar a operação, o usuário deve confirmar. Logo após será mostrada uma tela com o resultado da operação.

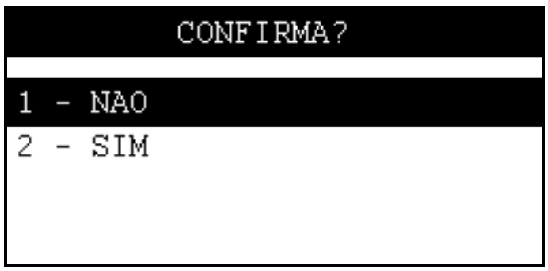


Figura 134 – Confirmação de Agendamento de manutenção

9.13 Menu Listas

Neste menu podem ser recolhidas as listas com dados relativos a ponto, acesso e auditoria.

9.13.1 Ponto/Acesso

Para realizar a coleta dos dados, primeiramente o usuário deve inserir a mídia na entrada USB presente na lateral do equipamento (vide seção 9.2 – Entrada USB). Após a inserção basta confirmar a gravação e esperar a finalização da operação.

O TEMPO LEVADO PARA GRAVAÇÃO DEPENDE DA QUANTIDADE DE DADOS QUE SERÃO RETIRADOS DO DISPOSITIVO, E DURANTE A GRAVAÇÃO O USUÁRIO DEVE EVITAR A RETIRADA DA MÍDIA DE ARMAZENAMENTO, SOB PENA DE DANIFICAR OS DADOS RETIRADOS DO DISPOSITIVO.

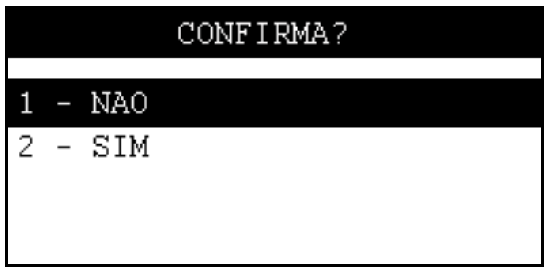


Figura 135 – Tela de confirmação de gravação de lista de ponto/acesso

Após a confirmação será mostrada uma tela com o resultado da operação, para sair desta tela o usuário deve retirar o dispositivo.

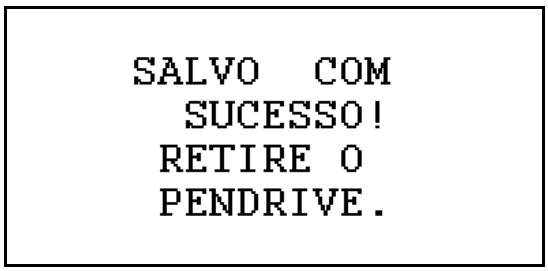


Figura 136 – Tela de sucesso na realização da gravação da lista de ponto/acesso

Após a coleta dos dados, e da retirada do pendrive o usuário pode encontrar os dados coletados na pasta timesheet no diretório raiz do mesmo.

Cada arquivo tem o nome composto pelo nome do equipamento, nome do local e a data de coleta, ou seja possui o formato "**LOCAL_IDEQUIP_time_sheet_list-DDMMAAAA.txt**" aonde:

LOCAL – Localidade do dispositivo

IDEQUIP – Identificador do dispositivo

DD – dia do mês

MM - mês

AAAA – ano

Para mais informações sobre como alterar o Id e local de dispositivo, consultar a seção 9.11.7 - ID do equipamento.

Dentro de cada arquivo os dados são listados por linha, e cada linha representa um acesso ou ponto coletado.

Os dados estão dispostos da seguinte maneira em cada linha:

01	EQUIP_01	08:00	12052010	0001	0004
Função (ponto/acesso)	Id de Equipamento	Horário de Ocorrência	Data de Ocorrência	Sequencial	Id do Usuário

- Função - identifica qual entrada foi feita, para ponto este campo será o e para acesso será 1.

- Id de Equipamento – Identifica o dispositivo no qual foi registrada a ocorrência.

- Horário de ocorrência – Marca o horário quando foi registrada a entrada.

- Data de Ocorrência – Marca a data de quando foi registrada a entrada, no formato AAAAMMDD.

- Sequencial – indica o número da ocorrência, somente é zerado quando é feita a limpeza dos registros de ponto e acesso.

- ID de usuário – Usuário para o qual foi criado o registro.

9.13.2 Limpar Ponto/Acesso

Esta função serve para limpar os dados relativos a ponto e acesso já gravados no dispositivo.

Para apagar os dados basta confirmar a exclusão.

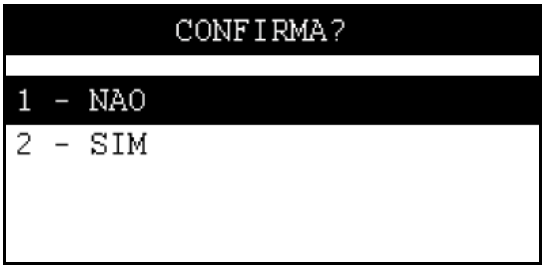


Figura 137 – Tela de confirmação de exclusão de eventos de ponto/acesso

Após a confirmação será mostrada uma tela com o resultado da operação.

9.13.3 Auditoria

A coleta de eventos de auditoria cria uma lista contendo as informações relativas a auditoria do sistema, de modo que um administrador possa ser capaz de observar quem alterou ou acessou o sistema.

Quando finalizada a coleta, será criada uma pasta de nome "events" no diretório raiz do dispositivo de armazenamento. Dentro desta pasta estará a lista coletada com as informações de eventos de auditoria do dispositivo.

O nome do arquivo deverá ter o seguinte formato:

Event list - DDMMAAAA-hhmmss.txt

Aonde:

DD – Dia do mês de coleta da lista

MM – Mês de coleta da lista

AAAA - Ano de coleta da lista

hh – Hora de coleta

mm – Minuto de coleta

ss – segundo de coleta

Dentro do arquivo estarão as informações, cada evento corresponde a uma linha do arquivo, e cada linha tem as informações mostradas da seguinte forma:

0001 EQUIP_01 0004 0004 2010-05-14 10:20:57 ENTRADA ACESSO PERMITIDO (MENU)

SEQUENCIAL	ID EQUIPAMENTO	USUARIO ORIGEM	USUARIO DESTINO	DATA/HORA	EVENTO	EXTENSÃO

Aonde:

SEQUENCIAL – Sequência de ocorrência do evento

ID EQUIPAMENTO – Identificação do equipamento aonde ocoreu o evento

USUARIO ORIGEM – Usuário que gerou o evento

USUARIO DESTINO – Caso exista, usuário que foi alvo da operação que gerou o evento

DATA/HORA – Data e hora de ocorrência do evento

EVENTO – Descrição do evento (pode ser uma operação ou evento de acesso)

EXTENSÃO – Descrição extendida da operação, para maior detalhamento caso necessário

Para realizar a coleta dos dados de auditoria, primeiramente o usuário deve inserir a mídia na entrada USB presente na lateral do equipamento (vide seção 9.2 – Entrada USB). Após a inserção basta confirmar a gravação e esperar a finalização da operação.

O tempo levado para gravação depende da quantidade de dados que serão retirados do dispositivo.

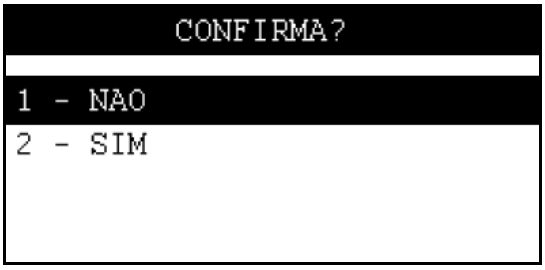


Figura 138 – Tela de confirmação de gravação de lista de auditoria

Após a confirmação será mostrada uma tela com o resultado da operação, para sair desta tela o usuário deve retirar o dispositivo.

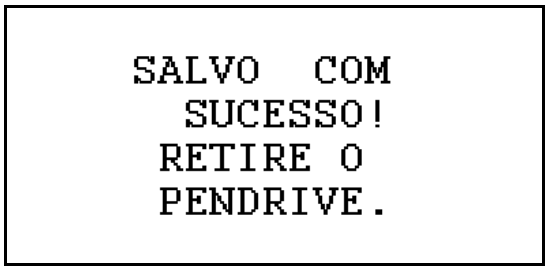


Figura 139 – Tela de sucesso na realização da gravação da lista de auditoria

10 Resolução de Problemas

Nesta seção encontram-se listados alguns problemas mais comuns. Recomenda-se ao usuário a leitura na íntegra deste documento a fim de conhecer melhor as capacidades e limitações do dispositivo, evitando problemas na utilização do mesmo.

10.1.1.1 *Dispositivo não liga*

Verifique se o dispositivo se encontra devidamente ligado á fonte de energia. Caso esteja, verifique se a fonte de energia está ligada. Para maiores informações, consultar a seção 7(Instalação e Cuidados).

Se o problema persistir contate a assistência técnica.

10.1.1.2 *Acionamento das saídas não funciona*

Verificar:

- Se a configuração das saídas está correta, verificando se o tempo de acionamento é suficiente e se o modo de acionamento é o correto,
- Se as conexões para o acionamento desejado estão corretas,
- Existem duas saídas solenóides disponíveis, verifique se a saída desejada é a que está ligada.

Para maiores informações, consultar a seção 7 (Instalação e Cuidados).

Se o problema persistir, contate a assistência técnica.

10.1.1.3 *Acesso negado em usuário cadastrado*

Verificar:

- Se dados utilizados para identificação foram os mesmos cadastrados para o usuário,
- Data e Horário de acesso do usuário, um usuário não pode ter acesso fora de seu horário,
- Se existe data de feriado cadastrada ou se o dispositivo não está bloqueado,

Para maiores informações, consultar as seções 9.12(Menu Cadastro, nas seções de inclusão de usuários e cadastro de datas).

Se o problema persistir, contate a assistência técnica.

10.1.1.4 *Botao não funciona*

Verificar:

- Conexões de entrada e circuito do botão,
- Configurações de Botao,
- Opção de status da porta,

Para maiores informações, consultar as seções 7.1.4 - Botão, 9.11.3 - Menu Saídas seção Botão.

Se o problema persistir, contate a assistência técnica.

10.1.1.5 Falha ao conseguir IP

Verificar:

- Se o cabo de rede se encontra ligado ao dispositivo,

- Se existe conexão de rede,

- Se a configuração da sua rede não suportar DHCP para IP dinâmico, o dispositivo deve ser configurado para utilização de IP estático,

- Parâmetros de rede configurados no dispositivo, caso o dispositivo esteja configurado para utilização de IP estático,

Para maiores informações, consultar a seção 9.10.4 - Menu REDE.

Se o problema persistir, contate a assistência técnica.

10.1.1.6 Data e Hora errados

Verificar:

- O dispositivo pode não ter sido configurado com a hora correta, refazer o procedimento de alteração de data/hora do dispositivo.

Para maiores informações, consultar a seção 9.10.3.1 - Alterar Data/Hora.

Se o problema persistir, contate a assistência técnica.

10.1.1.7 O acesso é permitido mas a porta não abre

Verificar:

- Se a fechadura está configurada corretamente,

- Se a saída correta foi associada á fechadura,

- Se o tempo de acionamento é suficiente,

- O dispositivo pode não estar configurado para funcionar como acesso,

Para maiores informações, consultar a seção 9.11.3(Menu Saídas, seção Fechadura), seção 9.11.2(Modo de Operação).

Se o problema persistir, contate a assistência técnica.

10.1.1.8 Ao realizar uma operação envolvendo um dispositivo de armazenamento USB o dispositivo trava na tela "RETIRE O PENDRIVE"

Para finalizar este tipo de operação, é requerido que o usuário retire a mídia USB para poder continuar utilizando o dispositivo. Enquanto o dispositivo estiver na entrada lateral o equipamento continuará nesta tela.

Caso o dispositivo apresente algum problema não listado nesta seção em seu funcionamento, favor contactar a assistência técnica.

digicon

EMPRESA ISO 9001:2000 CERTIFICADA

SEDE: Rua Nissin Castiel, 640 • Distrito Industrial
Cep: 94000-970 • Gravataí • RS • Brasil
Fone: +55 51 3489.8737

FILIAL: Rua São Paulo, 82 • Alphaville
Cep: 06465-130 • Barueri • SP
Fone: +55 11 4133.4100 • Fax: + 55 11 4191.2585

e-mail: vendas.acesso@digicon.com.br
www.digicon.com.br

A DIGICON reserva-se o direito de alterar as características destes equipamentos sem aviso prévio.

+DI.0XX.01-Mai/09